

10/069112

PCT/JP00/05770

日 本 国 特 許 庁

13.09.00

PATENT OFFICE  
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日  
Date of Application:

1999年12月 3日

REC'D 06 NOV 2000

出 願 番 号  
Application Number:

平成11年特許願第345229号

WIPO PCT

出 願 人  
Applicant (s):

富士通株式会社  
株式会社日立製作所  
日本コロムビア株式会社  
三洋電機株式会社

JP 00/05770  
+

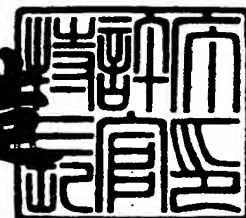
PRIORITY  
DOCUMENT

SUBMITTED OR TRANSMITTED IN  
COMPLIANCE WITH RULE 17.1(a) OR (b)

2000年10月20日

特許庁長官  
Commissioner,  
Patent Office

及 川 耕 造



出証番号 出証特2000-3085442

【書類名】	特許願
【整理番号】	1991488
【提出日】	平成11年12月 3日
【あて先】	特許庁長官殿
【国際特許分類】	H04M 11/08
【発明者】	
【住所又は居所】	神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内
【氏名】	畑中 正行
【発明者】	
【住所又は居所】	神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内
【氏名】	蒲田 順
【発明者】	
【住所又は居所】	神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内
【氏名】	畠山 卓久
【発明者】	
【住所又は居所】	神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内
【氏名】	長谷部 高行
【発明者】	
【住所又は居所】	神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内
【氏名】	小谷 誠剛
【発明者】	
【住所又は居所】	神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内
【氏名】	古田 茂樹

【発明者】

【住所又は居所】 東京都小平市上水本町5丁目20番1号 株式会社日立製作所 半導体グループ内

【氏名】 木下 泰三

【発明者】

【住所又は居所】 東京都港区赤坂四丁目14番14号 日本コロムビア株式会社内

【氏名】 穴澤 健明

【発明者】

【住所又は居所】 大阪府守口市京阪本通2丁目5番5号 三洋電機株式会社内

【氏名】 日置 敏昭

【発明者】

【住所又は居所】 大阪府守口市京阪本通2丁目5番5号 三洋電機株式会社内

【氏名】 金森 美和

【発明者】

【住所又は居所】 大阪府守口市京阪本通2丁目5番5号 三洋電機株式会社内

【氏名】 堀 吉宏

【特許出願人】

【識別番号】 000005223

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号

【氏名又は名称】 富士通株式会社

【特許出願人】

【識別番号】 000005108

【住所又は居所】 東京都千代田区神田駿河台4丁目6番地

【氏名又は名称】 株式会社日立製作所

【特許出願人】

【識別番号】 000004167

【住所又は居所】 東京都港区赤坂四丁目 1 4 番 1 4 号

【氏名又は名称】 日本コロムビア株式会社

【特許出願人】

【識別番号】 000001889

【住所又は居所】 大阪府守口市京阪本通 2 丁目 5 番 5 号

【氏名又は名称】 三洋電機株式会社

【代理人】

【識別番号】 100064746

【弁理士】

【氏名又は名称】 深見 久郎

【選任した代理人】

【識別番号】 100085132

【弁理士】

【氏名又は名称】 森田 俊雄

【選任した代理人】

【識別番号】 100091409

【弁理士】

【氏名又は名称】 伊藤 英彦

【選任した代理人】

【識別番号】 100096781

【弁理士】

【氏名又は名称】 堀井 豊

【先の出願に基づく優先権主張】

【出願番号】 平成11年特許願第241747号

【出願日】 平成11年 8月27日

【手数料の表示】

【予納台帳番号】 008693



【納付金額】

21,000円

【提出物件の目録】

【物件名】

明細書 1

【物件名】

図面 1

【物件名】

要約書 1

【プルーフの要否】

要

【書類名】 明細書

【発明の名称】 データ配信システム

【特許請求の範囲】

【請求項 1】 コンテンツデータ供給装置から、暗号化コンテンツデータを複数のユーザの各端末に配信するためのデータ配信システムであって、

前記コンテンツデータ供給装置は、

外部との間でデータを授受するための第 1 のインターフェース部と

前記暗号化コンテンツデータの通信ごとに更新される第 1 の共通鍵を生成する第 1 のセッションキー発生部と、

前記ユーザの端末に対応して予め定められた第 1 の公開暗号化鍵により前記第 1 の共通鍵を暗号化して前記第 1 のインターフェース部に与えるためのセッションキー暗号化部と、

前記第 1 の共通鍵により暗号化されて返信されるデータを復号するためのセッションキー復号部と、

前記暗号化コンテンツデータを復号するためのライセンスキーを、前記セッションキー復号部により復号されたデータを鍵データとして暗号化するための第 1 のライセンスデータ暗号化処理部と、

前記第 1 のライセンスデータ暗号化処理部の出力を第 2 の共通鍵でさらに暗号化して前記第 1 のインターフェース部に与え配信するための第 2 のライセンスデータ暗号化処理部とを備え、

各前記端末は、

外部との間でデータを授受するための第 2 のインターフェース部と、

前記暗号化コンテンツデータを受けて格納する配信データ解読部とを備え、

前記配信データ解読部は、

前記第 1 の公開暗号化鍵によって暗号化されたデータを復号化するための第 1 の秘密復号鍵を保持する第 1 の鍵保持部と、

前記第 1 の公開暗号化鍵によって暗号化された前記第 1 の共通鍵を受けて、復号処理するための第 1 の復号処理部と、

第 2 の公開暗号化鍵を保持するための第 2 の鍵保持部と、

前記第 2 の公開暗号化鍵を、前記第 1 の共通鍵に基づいて暗号化し、前記第 2 のインターフェース部に出力するための第 1 の暗号化処理部と、

前記第 2 のライセンスデータ暗号化処理部からの暗号化されたライセンスキーを受け、前記第 2 の共通鍵に基づいて復号化するための第 2 の復号処理部と、

前記第 2 の復号処理部の出力を受けて、格納するための第 1 の記憶部と、

前記第 2 の公開暗号化鍵によって暗号化されたデータを復号化するための第 2 の秘密復号鍵を保持する第 3 の鍵保持部と、

前記第 1 の記憶部に格納されたデータに基づいて、前記第 2 の秘密復号鍵により前記ライセンスキーを復号するための第 3 の復号処理部とを備える、データ配信システム。

【請求項 2】 前記配信データ解読部は、前記端末に着脱可能なメモリカードであり、

前記第 1 の秘密復号鍵は、前記メモリカードの種類に対応して予め定められた鍵であり、

前記第 2 の秘密復号鍵は、前記メモリカードごとに異なる、請求項 1 記載のデータ配信システム。

【請求項 3】 前記第 2 および第 3 の復号処理部は、前記コンテンツデータ供給装置において前記第 2 の公開暗号化鍵で暗号化され、さらに前記第 2 の共通鍵で暗号化されて、前記ライセンスキーとともに配信されるライセンス情報データを前記第 2 のインターフェース部を介して受け、前記第 2 の共通鍵および前記第 2 の秘密復号鍵に基づいて復号し、

前記配信データ解読部は、

復号された前記ライセンス情報データを格納する第 2 の記憶部をさらに備える、請求項 2 記載のデータ配信システム。

【請求項 4】 前記第 1 の共通鍵と前記第 2 の共通鍵とは、前記暗号化コンテンツデータの通信の際に、前記第 1 のセッションキー発生部により生成された同一の鍵データである、請求項 3 記載のデータ配信システム。

【請求項 5】 前記第 1 の記憶部は、前記ライセンスキーに基づいて復号できる前記暗号化コンテンツデータを前記コンテンツデータ供給装置から受けて格

納し、

前記配信データ解読部は、

外部から指示される再生動作モードに応じて、前記第 2 の記憶部に格納されたライセンス情報データにより再生可能かを判断して、前記配信データ解読部の動作を制御するための制御部をさらに備え、

前記第 1 の暗号化処理部は、前記制御部に制御されて、前記コンテンツデータの再生動作が指示されるのに応じて、前記第 3 の復号処理部からの前記ライセンスキーを受けて、第 3 の共通鍵に基づいて暗号化して出力し、

前記第 1 の記憶部は、前記制御部に制御されて、前記コンテンツデータの再生動作が指示されるのに応じて、前記暗号化コンテンツデータを出力し、

各前記端末は、

前記暗号化コンテンツデータの通信ごとに更新される前記第 3 の共通鍵を生成する第 2 のセッションキー発生部と、

前記配信データ解読部からの前記第 3 の共通鍵により暗号化された前記ライセンスキーを受けて復号して抽出し、前記第 1 の記憶部から出力された前記暗号化コンテンツデータを前記ライセンスキーにより復号して再生するコンテンツデータ再生部とをさらに備える、請求項 4 記載のデータ配信システム。

【請求項 6】 前記配信データ解読部は、

外部から指示される他の端末に前記暗号化コンテンツキーおよび前記ライセンス情報データを移転するための移動動作モードに応じて、前記配信データ解読部の動作を制御するための制御部と、

第 3 の公開暗号化鍵で暗号化処理を行なうための第 2 の暗号化処理部とをさらに含み、

前記第 2 の復号処理部は、前記制御部に制御されて、前記移動動作モードが指定されるのに応じて、前記第 3 の共通鍵に基づいて暗号化されて前記他の端末の側から送信される前記第 3 の公開暗号化鍵を復号して抽出し、

前記第 2 の暗号化処理部は、前記移動動作モードが指定されるのに応じて、前記ライセンスキーおよび前記ライセンス情報データを前記第 3 の公開暗号化鍵で暗号化し、

前記第 1 の暗号化処理部は、前記第 2 の暗号化処理部の出力を受けて、前記第 3 の共通鍵に基づいて暗号化して前記第 2 のインターフェース部に与え、

前記制御部は、前記移動動作モードが指定されるのに応じて、前記第 2 の記憶部に格納されている前記ライセンス情報データを消去し、

前記第 1 の記憶部は、前記移動動作モードが指定されるのに応じて、前記暗号化コンテンツデータを前記第 2 のインターフェース部に与える、請求項 5 記載のデータ配信システム。

【請求項 7】 前記配信データ解読部は、

外部から指示される他の端末に前記暗号化コンテンツデータを移転するための複製動作モードに応じて、前記配信データ解読部の動作を制御するための制御部をさらに含み、

前記第 1 の記憶部は、前記複製動作モードが指定されるのに応じて、前記暗号化コンテンツデータを前記第 2 のインターフェース部に与える、請求項 5 記載のデータ配信システム。

【請求項 8】 前記配信データ解読部は、

前記第 2 の共通鍵を生成するための第 3 のセッションキー発生部と、

前記第 3 のセッションキー発生部の出力を暗号化して前記第 2 のインターフェース部に与えることが可能な第 3 の暗号化処理部とをさらに含む、請求項 3 記載のデータ配信システム。

【請求項 9】 前記第 1 の記憶部は、前記ライセンスキーに基づいて復号できる前記暗号化コンテンツデータを前記コンテンツデータ供給装置から受けて格納し、

前記配信データ解読部は、

外部から指示される再生動作モードに応じて、前記第 2 の記憶部に格納されたライセンス情報データにより再生可能かを判断して、前記配信データ解読部の動作を制御するための制御部をさらに備え、

前記第 3 の暗号化処理部は、第 4 の公開暗号化鍵により前記第 3 のセッションキー発生部の出力を暗号化して前記第 2 のインターフェース部に与え、

前記第 1 の暗号化処理部は、前記制御部に制御されて、前記コンテンツデータ

の再生動作が指示されるのに応じて、前記第3の復号処理部からの前記ライセンスキーを受けて、第3の共通鍵に基づいて暗号化して出力し、

前記第1の記憶部は、前記制御部に制御されて、前記コンテンツデータの再生動作が指示されるのに応じて、前記暗号化コンテンツデータを出力し、

各前記端末は、

前記暗号化コンテンツデータの通信ごとに更新される前記第3の共通鍵を生成する第2のセッションキー発生部と、

前記第4の公開暗号化鍵を前記配信データ解読部に与える公開鍵保持部と、

前記第4の公開暗号化鍵で暗号化された前記第2の共通鍵を復号可能な公開鍵復号部と、

前記配信データ解読部からの前記第3の共通鍵により暗号化された前記ライセンスキーを受けて復号して抽出し、前記第1の記憶部から出力された前記暗号化コンテンツデータを前記ライセンスキーにより復号して再生するコンテンツデータ再生部とをさらに備える、請求項8記載のデータ配信システム。

【請求項10】 前記配信データ解読部は、

外部から指示される他の端末に前記暗号化コンテンツデータおよび前記ライセンス情報データを移転するための移動動作モードに応じて、前記配信データ解読部の動作を制御するための制御部と、

第3の公開暗号化鍵で暗号化処理を行なうための第2の暗号化処理部とをさらに含み、

前記第2の復号処理部は、前記制御部に制御されて、前記移動動作モードが指定されるのに応じて、前記第3の共通鍵に基づいて暗号化されて前記他の端末の側から送信される前記第3の公開暗号化鍵を復号して抽出し、

前記第2の暗号化処理部は、前記移動動作モードが指定されるのに応じて、前記ライセンスキーおよび前記ライセンス情報データを前記第3の公開暗号化鍵で暗号化し、

前記第1の暗号化処理部は、前記第2の暗号化処理部の出力を受けて、前記第3の共通鍵に基づいて暗号化して前記第2のインターフェース部に与え、

前記制御部は、前記移動動作モードが指定されるのに応じて、前記第2の記憶

部に格納されている前記ライセンス情報データを消去し、

前記第 1 の記憶部は、前記移動動作モードが指定されるのに応じて、前記暗号化コンテンツデータを前記第 2 のインターフェース部に与える、請求項 9 記載のデータ配信システム。

【請求項 1 1】 前記配信データ解読部は、

外部から指示される他の端末に前記暗号化コンテンツデータを移転するための複製動作モードに応じて、前記配信データ解読部の動作を制御するための制御部をさらに含み、

前記第 1 の記憶部は、前記複製動作モードが指定されるのに応じて、前記暗号化コンテンツデータを前記第 2 のインターフェース部に与える、請求項 9 記載のデータ配信システム。

【請求項 1 2】 前記第 1 のインターフェース部と前記第 2 のインターフェース部とは、携帯電話網により接続され、

前記コンテンツデータ供給装置は、

前記第 1 の公開暗号鍵に基づいて、前記ユーザの認証を行なう、請求項 1 記載のデータ配信システム。

【請求項 1 3】 前記第 1 のインターフェース部は、

前記端末と直接接続可能なコネクタ部を含む、請求項 1 記載のデータ配信システム。

【請求項 1 4】 前記第 1 のインターフェース部は、

前記メモリーカードと直接接続可能な接続部を含む、請求項 2 記載のデータ配信システム。

【請求項 1 5】 コンテンツデータ供給装置から、暗号化コンテンツデータと前記暗号化データを復号するためのコンテンツキーとのうちの少なくとも 1 つを複数のユーザの各端末に配信するためのデータ配信システムであって、

前記コンテンツデータ供給装置は、

外部との間でデータを授受するための第 1 のインターフェイス部と、

前記暗号化コンテンツデータの通信ごとに更新される第 1 の共通鍵を生成する第 1 のセッションキー発生部と、

前記ユーザの端末に対応して予め定められた第 1 の公開暗号化鍵により前記第 1 の共通鍵を暗号化して前記第 1 のインターフェイス部に与えるためのセッションキー暗号化処理部と、

前記第 2 の共通鍵により暗号化されて返信される第 2 の共通鍵と第 2 の公開暗号化鍵を復号し抽出するセッションキー復号部と、

前記暗号化コンテンツデータを復号するためのコンテンツキーを、前記セッションキー復号部により復号された第 2 の公開暗号化鍵により暗号化するための第 1 のライセンスデータ暗号化処理部と、

前記第 1 のライセンスデータ暗号化処理部の出力を前記第 2 の共通鍵でさらに暗号化して前記第 1 のインターフェイス部に与え配信するための第 2 のライセンス暗号化処理部とを備え、

各前記端末は、

外部との間でデータを授受するための第 2 のインターフェイス部と、

前記暗号化コンテンツデータおよび前記コンテンツキーを受けて格納する配信データ解読部とを備え、

前記配信データ解読部は、

前記第 1 の公開暗号化鍵によって暗号化されたデータを復号化するための第 1 の秘密復号鍵を保持する第 1 の鍵保持部と、

前記第 1 の公開暗号化鍵によって暗号化された前記第 1 の共通鍵を受けて、復号処理するための第 1 の復号処理部と、

第 2 の公開暗号化鍵を保持するための第 2 の鍵保持部と、

第 2 の共通鍵を生成する第 2 のセッションキー発生部と、

前記第 2 の公開暗号化鍵と前記第 2 の共通鍵を、前記第 1 の共通鍵に基づいて暗号化し、前記第 2 のインターフェイス部に出力するための第 1 の暗号化処理部と、

前記第 2 のライセンスデータ暗号化処理部からの暗号化されたコンテンツキーを受け、前記第 2 の共通鍵に基づいて復号するための第 2 の復号処理部と、

前記第 2 の復号処理部の出力と、前記コンテンツキーにて復号可能な暗号化コンテンツデータを格納するための記憶部と、



前記第 2 の公開暗号化鍵によって暗号化されたデータを復号化するための第 2 の秘密復号鍵を保持する第 3 の鍵保持部と、

前記記憶部に格納されたデータに基づいて、前記第 2 の秘密復号鍵により前記コンテンツキーを復号し抽出するための第 3 の復号処理部と、

前記第 1 の公開暗号化鍵を少なくとも含む第 1 の認証データを公開認証鍵により復号できるように暗号化して保持し外部に出力可能な第 1 の認証データ保持部と、

前記公開認証鍵により復号できる外部から与えられる第 1 の認証データを復号して抽出するための第 1 の認証復号処理部とを備え、

前記コンテンツデータ供給部は、

前記第 1 の認証復号処理部により抽出された前記第 1 の認証データに基づいて認証処理を行ない、少なくともコンテンツキーを配信するか否かを判断する配信制御手段をさらに含む、データ配信システム。

【請求項 1 6】 前記配信データ解読部は、前記端末に着脱可能なメモリカードであり、

前記第 1 の秘密復号鍵は、前記メモリカードの種類に対応して予め定められた値であり

前記第 2 の秘密復号鍵は、前記メモリカードごとに異なる、請求項 1 5 記載のデータ配信システム。

【請求項 1 7】 各前記端末は、コンテンツ再生部をさらに備え、

前記コンテンツ再生部は、

予め定められた第 3 の公開暗号化鍵を少なくとも含む第 2 の認証データを前記公開認証鍵に基づいて復号できるように暗号化して保持し、外部に対して出力できる第 2 の認証データ保持部をさらに含む、請求項 1 5 記載のデータ配信システム。

【請求項 1 8】 前記第 1 の認証復号処理部は、

前記公開認証鍵により復号できるように暗号化された第 2 の認証データをさらに復号して出力し、

前記配信制御部は、

前記第1の認証復号処理部にて抽出された前記第1の認証データおよび前記第2の認証データに基づいて認証処理を行ない、少なくともコンテンツキーを配信するか否かを判断する、請求項17に記載のデータ配信システム。

【請求項19】 前記第1のインタフェイス部と前記第2のインタフェイス部とは、携帯電話網により接続される、請求項15記載のデータ配信システム。

【請求項20】 前記第1のインタフェイス部は、前記端末と直接接続可能なコネクタ部を含む、請求項15記載のデータ配信システム。

【請求項21】 前記第1のインタフェイス部は、前記データ格納部と直接接続可能な接続部を含む、請求項16記載のデータ配信システム。

【請求項22】 前記データ解読部は、前記接続部からのデータを受ける複数の端子を含み、外部からの指令に従って、前記接続部からデータを受ける端子数が切換え可能である、請求項21記載のデータ配信システム。

【請求項23】 前記データ再生部は、前記第3の公開暗号鍵にて暗号化されたデータを復号する第3の秘密復号鍵を保持するための第4の鍵保持部と、

外部にて前記第3の公開暗号化鍵によって暗号化された第2の共通鍵を復号し抽出するための第3の復号処理部と、

第3の共通鍵を生成する第3のセッションキー発生部と、

前記第3の復号処理部にて復号し抽出した前記第2の共通鍵に基づいて、前記第3の共通鍵を暗号化し出力するための第2の暗号化処理部と、

外部にて前記第3の共通鍵に基づいて暗号化されたコンテンツキーを復号し抽出するための第4復号処理部と、

前記記録部に記録された暗号化コンテンツデータを抽出した前記コンテンツキーにて復号し、再生するためのデータ再生部とをさらに備え、

配信データ解読部は、

前記公開認証鍵により復号できる前記コンテンツ再生部からの与えられる暗号

化された第2の認証データを復号して前記第3の公開鍵を抽出するための第2の認証復号処理部と、

前記第2のセッションキー発生部にて生成した第2の共通鍵を前記第3の公開暗号化鍵に基づいて暗号化する第3の暗号化処理部と、

前記データ再生部にて前記第2の共通鍵にて暗号化された前記第3の共通鍵を受けて、前記第1の復号処理部にて前記第2の共通鍵に基づいて復号した前記第3の共通鍵に基づいて、前記記録部に格納されたデータを前記第2の秘密復号鍵にて復号した前記コンテンツキーを、前記第1の暗号化処理部にて暗号化し、前記コンテンツ再生部へ出力を指示する制御部とをさらに備え、

前記制御手段は、前記第2の認証復号処理部により復号された前記第2の認証データに基づいて認証処理を行ない、少なくともコンテンツキーを出力するか否かを判断する、請求項17記載のデータ配信システム。

【請求項24】 前記配信データ解読部は、

前記第2の公開鍵によって前記第2の共通鍵を暗号化するための第4の暗号化処理部をさらに含み、

前記認証復号処理部は、外部から指示される、他の配信データ解読部に少なくとも前記コンテンツキーを移転する移動処理に応じて、前記他のデータ解読部の前記公開認証鍵によって復号できる暗号化された第1の認証データを、前記公開認証鍵にて復号して、前記他のデータ解読部における第1の公開暗号化鍵を抽出し、

前記第2のセッションキー発生部は、前記移動処理に応じて、前記第2の共通鍵を発生し、

前記第3の暗号化処理部は、前記移動処理に応じて、前記他の配信データ解読部の第1の公開暗号化鍵に基づいて、前記第2の共通鍵を暗号化し、

前記第2の復号処理部は、前記移動処理に応じて、前記他の配信データ解読部から前記第2の共通鍵によって暗号化され、入力される第4の共通鍵と他の配信データ解読部の第2の公開暗号化鍵とを復号して抽出し、

前記第3の復号処理部は、前記移動処理に応じて、第2の秘密復号鍵に基づいて、前記記録部に格納された第2の公開暗号化鍵にて暗号化されたデータを復号

し、コンテンツキーを抽出し、

前記第 4 の暗号化処理部は、前記移動処理に応じて、前記他のメモ리카ードの第 2 の公開暗号化鍵に基づいて、抽出された前記コンテンツキーを暗号化し、

前記第 1 の暗号化処理部は、前記移動処理に応じて、前記第 4 の暗号化処理部の出力を前記第 4 の共通鍵にて暗号化し、前記他の配信データ解読部に対して出力し、

前記制御手段は、前記第 2 の認証復号処理部により抽出された前記他のデータ解読部から出力された第 2 の認証データに基づき認証処理を行ない、少なくともコンテンツキーを出力するか否かを判断する、請求項 1 6 記載のデータ配信システム。

【請求項 2 5】 前記配信データ解読部は、

前記認証復号処理は、外部から指示される、他の配信データ解読部から少なくとも前記コンテンツキーを移転する移動受理処理に応じて、前記第 2 の認証データ保持部が前記第 2 の認証データを出力し、

前記第 1 の復号処理部は、前記移動受理処理に応じて、前記他の配信データ解読部から前記第 1 の公開暗号化鍵によって暗号化され、入力される前記他の配信データ解読部にて発生された前記第 4 の共通鍵を復号して抽出し、

前記第 2 のセッションキー発生部は、前記移動受理処理に応じて、第 2 の共通鍵を発生し、

前記第 1 の暗号化処理部は、前記移動受理処理に応じて、第 4 の共通鍵に基づいて、前記第 2 の公開暗号化鍵と前記第 2 の共通鍵とを暗号化して出力し、

前記第 2 の復号処理部は、前記他の配信データ解読部に前記第 2 の公開暗号化鍵にて暗号化され、さらに前記第 2 の共通鍵にて暗号化されたコンテンツキーを前記第 2 の共通鍵にて復号し、前記記録部に記録する請求項 2 2 記載のデータ配信システム。

【請求項 2 6】 前記コンテンツデータ供給装置は、

前記コンテンツ再生部と共通な第 5 の共通鍵を保持する第 5 の鍵保持部と、

前記第 5 の鍵保持部に保持された前記第 5 の共通鍵に基づいて、前記コンテンツキーを暗号化し前記第 1 のライセンス暗号化処理部に対して出力する第 3 のラ

イセンス暗号化部をさらに含み、

前記コンテンツ再生部は、

前記第 5 の共通鍵を保持する第 6 の鍵保持手段と、

前記第 4 の復号処理部と前記データ再生部との間に設けられ、前記第 6 の鍵保持部に保持された前記第 5 の共通鍵によって、前記第 4 の復号処理部の出力から前記コンテンツキーを復号し抽出し、前記データ再生部に対して出力する第 5 の復号処理部をさらに含む、請求項 2 1 記載のデータ配信システム。

【請求項 2 7】 前記コンテンツデータ供給装置は、

前記コンテンツ再生部にて復号可能な第 4 の公開暗号化鍵を保持する第 5 の鍵保持部と、

第 4 の公開暗号化鍵に基づいて前記コンテンツキーを暗号化し前記第 1 のライセンス暗号化処理部にて出力する第 3 のライセンス暗号化部をさらに含み、

前記コンテンツ再生部は、

第 4 の公開暗号化鍵によって暗号化されたデータを復号できる第 4 の秘密復号鍵を保持する第 6 の鍵保持手段と、

前記第 4 の復号処理部と前記データ再生部との間に設けられ、第 4 の秘密復号鍵によって前記第 4 の復号処理部の出力から前記コンテンツキーを復号し抽出し、前記データ再生部に対して出力する第 5 の復号処理部をさらに含む、請求項 2 1 記載のデータ配信システム。

【請求項 2 8】 前記データ再生部は、

複数の配信データ解読部を備える、請求項 1 6 記載のデータ配信システム。

【発明の詳細な説明】 \_\_\_\_\_

【0 0 0 1】

【発明の属する技術分野】

本発明は、携帯電話等の端末に対して情報を配送するためのデータ配信システムに関し、より特定的には、コピーされた情報に対する著作権保護を可能とするデータ配信システムに関するものである。

【0 0 0 2】

【従来の技術】

近年、インターネット等の情報通信網等の進歩により、携帯電話等を用いた個人向け端末により、各ユーザが容易にネットワーク情報にアクセスすることが可能となっている。

【0003】

このような情報通信においてはデジタル信号により情報が伝送される。したがって、たとえば上述のような情報通信網において伝送された音楽や映像情報を各個人ユーザがコピーした場合でも、そのようなコピーによる音質や画質の劣化をほとんど生じさせることなく、情報のコピーを行なうことが可能である。

【0004】

したがって、このような情報通信網上において、音楽情報や画像情報等の著作権の存在する創作物が伝達される場合、適切な著作権保護のための方策が取られていないと、著しく著作権者の権利が侵害されてしまうおそれがある。

【0005】

一方で、著作権保護の目的を最優先して、急拡大するデジタル情報通信網を介して著作物データの配信を行なうことができないとすると、基本的には、著作物の複製に際して一定の著作権料を徴収することが可能な著作権者にとっても、かえって不利益となる。

【0006】

ここで、上述のようなデジタル情報通信網を介した配信ではなく、デジタル情報を記録した記録媒体を例にとって考えてみると、通常販売されている音楽情報を記録したCD（コンパクトディスク）については、CDから光磁気ディスク（MD等）への音楽データのコピーは、当該コピーした音楽を個人的な使用に止める限り原則的には自由に行なうことができる。ただし、デジタル録音等を行なう個人ユーザは、デジタル録音機器自体やMD等の媒体の代金のうちの一定額を間接的に著作権者に対して補償金として支払うことになっている。

【0007】

しかも、CDからMDへデジタル信号である音楽情報をコピーした場合、これらの情報がコピー劣化のほとんどないデジタル情報であることに鑑み、1つのMDからさらに他のMDに音楽データをデジタル情報としてコピーすることは、著

著作権保護のために機器の構成上できないようになっている。

【0008】

すなわち、現状においては、デジタル記録媒体であるCDからMDへのコピーは、親から子へのコピーは自由に行なうことができるものの、記録可能なMDからMDへのコピーを行なうことはできない。

【0009】

【発明が解決しようとする課題】

そのような事情からも、音楽データや画像データをデジタル情報通信網を通じて公衆に配信することは、それ自体が著作権者の公衆送信権による制限を受ける行為であるから、著作権保護のための十分な方策が講じられる必要がある。

【0010】

この場合、情報通信網を通じて公衆に送信される著作物データを、本来受信する権限のないユーザが受信することを防止する必要があるのはもちろんのこと、仮に権限を有するユーザが受信を行なった場合でも、一度受信された著作物が、さらに勝手に複製されることを防止することも必要となる。

【0011】

本発明は、上記のような問題点を解決するためになされたものであって、その目的は、情報通信網、たとえば携帯電話等の情報通信網を介して著作物データを配信する場合に、正当なアクセス権を有するユーザのみがこのような情報を受信することが可能な情報配信システムを提供することである。

【0012】

この発明の他の目的は、配信された著作物データが、著作権者の許可なく複製されることを防止することが可能な情報配信システムを提供することである。

【0013】

【課題を解決するための手段】

請求項1記載のデータ配信システムは、コンテンツデータ供給装置から、暗号化コンテンツデータを複数のユーザの各端末に配信するためのデータ配信システムであって、コンテンツデータ供給装置は、外部との間でデータを授受するための第1のインターフェース部と暗号化コンテンツデータの通信ごとに更新される

第1の共通鍵を生成する第1のセッションキー発生部と、ユーザの端末に対応して予め定められた第1の公開暗号化鍵により第1の共通鍵を暗号化して第1のインターフェース部に与えるためのセッションキー暗号化部と、第1の共通鍵により暗号化されて返信されるデータを復号するためのセッションキー復号部と、暗号化コンテンツデータを復号するためのライセンスキーを、セッションキー復号部により復号されたデータを鍵データとして暗号化するための第1のライセンスデータ暗号化処理部と、第1のライセンスデータ暗号化処理部の出力を第2の共通鍵でさらに暗号化して第1のインターフェース部に与え配信するための第2のライセンスデータ暗号化処理部とを備え、各端末は、外部との間でデータを授受するための第2のインターフェース部と、暗号化コンテンツデータを受けて格納する配信データ解読部とを備え、配信データ解読部は、第1の公開暗号化鍵によって暗号化されたデータを復号化するための第1の秘密復号鍵を保持する第1の鍵保持部と、第1の公開暗号化鍵によって暗号化された第1の共通鍵を受けて、復号処理するための第1の復号処理部と、第2の公開暗号化鍵を保持するための第2の鍵保持部と、第2の公開暗号化鍵を、第1の共通鍵に基づいて暗号化し、第2のインターフェース部に出力するための第1の暗号化処理部と、第2のライセンスデータ暗号化処理部からの暗号化されたライセンスキーを受け、第2の共通鍵に基づいて復号化するための第2の復号処理部と、第2の復号処理部の出力を受けて、格納するための第1の記憶部と、第2の公開暗号化鍵によって暗号化されたデータを復号化するための第2の秘密復号鍵を保持する第3の鍵保持部と、第1の記憶部に格納されたデータに基づいて、第2の秘密復号鍵によりライセンスキーを復号するための第3の復号処理部とを備える。

## 【0014】

請求項2記載のデータ配信システムは、請求項1記載のデータ配信システムの構成に加えて、配信データ解読部は、端末に着脱可能なメモリカードであり、第1の秘密復号鍵は、メモリカードの種類に対応して予め定められた鍵であり、第2の秘密復号鍵は、メモリカードごとに異なる。

## 【0015】

請求項3記載のデータ配信システムは、請求項2記載のデータ配信システムの



構成に加えて、第2および第3の復号処理部は、コンテンツデータ供給装置において第2の公開暗号化鍵で暗号化され、さらに第2の共通鍵で暗号化されて、ライセンスキーとともに配信されるライセンス情報データを第2のインターフェース部を介して受け、第2の共通鍵および第2の秘密復号鍵に基づいて復号し、配信データ解読部は、復号されたライセンス情報データを格納する第2の記憶部をさらに備える。

## 【0016】

請求項4記載のデータ配信システムは、請求項3記載のデータ配信システムの構成に加えて、第1の共通鍵と第2の共通鍵とは、暗号化コンテンツデータの通信の際に、第1のセッションキー発生部により生成された同一の鍵データである。

## 【0017】

請求項5記載のデータ配信システムは、請求項4記載のデータ配信システムの構成に加えて、第1の記憶部は、ライセンスキーに基づいて復号できる暗号化コンテンツデータをコンテンツデータ供給装置から受けて格納し、配信データ解読部は、外部から指示される再生動作モードに応じて、第2の記憶部に格納されたライセンス情報データにより再生可能かを判断して、配信データ解読部の動作を制御するための制御部をさらに備え、第1の暗号化処理部は、制御部に制御されて、コンテンツデータの再生動作が指示されるのに応じて、第3の復号処理部からのライセンスキーを受けて、第3の共通鍵に基づいて暗号化して出力し、第1の記憶部は、制御部に制御されて、コンテンツデータの再生動作が指示されるのに応じて、暗号化コンテンツデータを出力し、各端末は、暗号化コンテンツデータの通信ごとに更新される第3の共通鍵を生成する第2のセッションキー発生部と、配信データ解読部からの第3の共通鍵により暗号化されたライセンスキーを受けて復号して抽出し、第1の記憶部から出力された暗号化コンテンツデータをライセンスキーにより復号して再生するコンテンツデータ再生部とをさらに備える。

## 【0018】

請求項6記載のデータ配信システムは、請求項5記載のデータ配信システムの

構成に加えて、配信データ解読部は、外部から指示される他の端末に暗号化コンテンツキーおよびライセンス情報データを移転するための移動動作モードに応じて、配信データ解読部の動作を制御するための制御部と、第3の公開暗号化鍵で暗号化処理を行なうための第2の暗号化処理部とをさらに含み、第2の復号処理部は、制御部に制御されて、移動動作モードが指定されるのに応じて、第3の共通鍵に基づいて暗号化されて他の端末の側から送信される第3の公開暗号化鍵を復号して抽出し、第2の暗号化処理部は、移動動作モードが指定されるのに応じて、ライセンスキーおよびライセンス情報データを第3の公開暗号化鍵で暗号化し、第1の暗号化処理部は、第2の暗号化処理部の出力を受けて、第3の共通鍵に基づいて暗号化して第2のインターフェース部に与え、制御部は、移動動作モードが指定されるのに応じて、第2の記憶部に格納されているライセンス情報データを消去し、第1の記憶部は、移動動作モードが指定されるのに応じて、暗号化コンテンツデータを第2のインターフェース部に与える。

【0019】

請求項7記載のデータ配信システムは、請求項5記載のデータ配信システムの構成に加えて、配信データ解読部は、外部から指示される他の端末に暗号化コンテンツデータを移転するための複製動作モードに応じて、配信データ解読部の動作を制御するための制御部をさらに含み、第1の記憶部は、複製動作モードが指定されるのに応じて、暗号化コンテンツデータを第2のインターフェース部に与える。

【0020】

請求項8記載のデータ配信システムは、請求項3記載のデータ配信システムの構成に加えて、配信データ解読部は、第2の共通鍵を生成するための第3のセッションキー発生部と、第3のセッションキー発生部の出力を暗号化して第2のインターフェース部に与えることが可能な第3の暗号化処理部とをさらに含む。

【0021】

請求項9記載のデータ配信システムは、請求項8記載のデータ配信システムの構成に加えて、第1の記憶部は、ライセンスキーに基づいて復号できる暗号化コンテンツデータをコンテンツデータ供給装置から受けて格納し、配信データ解読

部は、外部から指示される再生動作モードに応じて、第2の記憶部に格納されたライセンス情報データにより再生可能かを判断して、配信データ解読部の動作を制御するための制御部をさらに備え、第3の暗号化処理部は、第4の公開暗号化鍵により第3のセッションキー発生部の出力を暗号化して第2のインターフェース部に与え、第1の暗号化処理部は、制御部に制御されて、コンテンツデータの再生動作が指示されるのに応じて、第3の復号処理部からのライセンスキーを受けて、第3の共通鍵に基づいて暗号化して出力し、第1の記憶部は、制御部に制御されて、コンテンツデータの再生動作が指示されるのに応じて、暗号化コンテンツデータを出力し、各端末は、暗号化コンテンツデータの通信ごとに更新される第3の共通鍵を生成する第2のセッションキー発生部と、第4の公開暗号化鍵を配信データ解読部に与える公開鍵保持部と、第4の公開暗号化鍵で暗号化された第2の共通鍵を復号可能な公開鍵復号部と、配信データ解読部からの第3の共通鍵により暗号化されたライセンスキーを受けて復号して抽出し、第1の記憶部から出力された暗号化コンテンツデータをライセンスキーにより復号して再生するコンテンツデータ再生部とをさらに備える。

#### 【0022】

請求項10記載のデータ配信システムは、請求項9記載のデータ配信システムの構成に加えて、配信データ解読部は、外部から指示される他の端末に暗号化コンテンツデータおよびライセンス情報データを移転するための移動動作モードに応じて、配信データ解読部の動作を制御するための制御部と、第3の公開暗号化鍵で暗号化処理を行なうための第2の暗号化処理部とをさらに含み、第2の復号処理部は、制御部に制御されて、移動動作モードが指定されるのに応じて、第3の共通鍵に基づいて暗号化されて他の端末の側から送信される第3の公開暗号化鍵を復号して抽出し、第2の暗号化処理部は、移動動作モードが指定されるのに応じて、ライセンスキーおよびライセンス情報データを第3の公開暗号化鍵で暗号化し、第1の暗号化処理部は、第2の暗号化処理部の出力を受けて、第3の共通鍵に基づいて暗号化して第2のインターフェース部に与え、制御部は、移動動作モードが指定されるのに応じて、第2の記憶部に格納されているライセンス情報データを消去し、第1の記憶部は、移動動作モードが指定されるのに応じて、

暗号化コンテンツデータを第2のインターフェース部に与える。

【0023】

請求項11記載のデータ配信システムは、請求項9記載のデータ配信システムの構成に加えて、配信データ解読部は、外部から指示される他の端末に暗号化コンテンツデータを移転するための複製動作モードに応じて、配信データ解読部の動作を制御するための制御部をさらに含み、第1の記憶部は、複製動作モードが指定されるのに応じて、暗号化コンテンツデータを第2のインターフェース部に与える。

【0024】

請求項12記載のデータ配信システムは、請求項1記載のデータ配信システムの構成に加えて、第1のインターフェース部と第2のインターフェース部とは、携帯電話網により接続され、コンテンツデータ供給装置は、第1の公開暗号鍵に基づいて、ユーザの認証を行なう。

【0025】

請求項13記載のデータ配信システムは、請求項1記載のデータ配信システムの構成に加えて、第1のインターフェース部は、端末と直接接続可能なコネクタ部を含む。

【0026】

請求項14記載のデータ配信システムは、請求項2記載のデータ配信システムの構成に加えて、第1のインターフェース部は、メモリーカードと直接接続可能な接続部を含む。

【0027】

請求項15記載のデータ配信システムは、コンテンツデータ供給装置から、暗号化コンテンツデータと暗号化データを復号するためのコンテンツキーとのうちの少なくとも1つを複数のユーザの各端末に配信するためのデータ配信システムであって、コンテンツデータ供給装置は、外部との間でデータを授受するための第1のインターフェイス部と、暗号化コンテンツデータの通信ごとに更新される第1の共通鍵を生成する第1のセッションキー発生部と、ユーザの端末に対応して予め定められた第1の公開暗号化鍵により第1の共通鍵を暗号化して第1のイ

ンターフェイス部に与えるためのセッションキー暗号化処理部と、第2の共通鍵により暗号化されて返信される第2の共通鍵と第2の公開暗号化鍵を復号し抽出するセッションキー復号部と、暗号化コンテンツデータを復号するためのコンテンツキーを、セッションキー復号部により復号された第2の公開暗号化鍵により暗号化するための第1のライセンスデータ暗号化処理部と、第1のライセンスデータ暗号化処理部の出力を第2の共通鍵でさらに暗号化して第1のインターフェイス部に与え配信するための第2のライセンス暗号化処理部とを備え、各端末は、外部との間でデータを授受するための第2のインターフェイス部と、暗号化コンテンツデータおよびコンテンツキーを受けて格納する配信データ解読部とを備え、配信データ解読部は、第1の公開暗号化鍵によって暗号化されたデータを復号化するための第1の秘密復号鍵を保持する第1の鍵保持部と、第1の公開暗号化鍵によって暗号化された第1の共通鍵を受けて、復号処理するための第1の復号処理部と、第2の公開暗号化鍵を保持するための第2の鍵保持部と、第2の共通鍵を生成する第2のセッションキー発生部と、第2の公開暗号化鍵と第2の共通鍵を、第1の共通鍵に基づいて暗号化し、第2のインターフェイス部に出力するための第1の暗号化処理部と、第2のライセンスデータ暗号化処理部からの暗号化されたコンテンツキーを受け、第2の共通鍵に基づいて復号するための第2の復号処理部と、第2の復号処理部の出力と、コンテンツキーにて復号可能な暗号化コンテンツデータを格納するための記憶部と、第2の公開暗号化鍵によって暗号化されたデータを復号化するための第2の秘密復号鍵を保持する第3の鍵保持部と、記憶部に格納されたデータに基づいて、第2の秘密復号鍵によりコンテンツキーを復号し抽出するための第3の復号処理部と、第1の公開暗号化鍵を少なくとも含む第1の認証データを公開認証鍵により復号できるように暗号化して保持し外部に出力可能な第1の認証データ保持部と、公開認証鍵により復号できる外部から与えられる第1の認証データを復号して抽出するための第1の認証復号処理部とを備え、コンテンツデータ供給部は、第1の認証復号処理部により抽出された第1の認証データに基づいて認証処理を行ない、少なくともコンテンツキーを配信するか否かを判断する配信制御手段をさらに含む。

【0028】

請求項 1 6 記載のデータ配信システムは、請求項 1 5 記載のデータ配信システムの構成に加えて、配信データ解読部は、端末に着脱可能なメモリカードであり、第 1 の秘密復号鍵は、メモリカードの種類に対応して予め定められた値であり第 2 の秘密復号鍵は、メモリカードごとに異なる。

## 【 0 0 2 9 】

請求項 1 7 記載のデータ配信システムは、請求項 1 5 記載のデータ配信システムの構成に加えて、各端末は、コンテンツ再生部をさらに備え、コンテンツ再生部は、予め定められた第 3 の公開暗号鍵を少なくとも含む第 2 の認証データを公開認証鍵に基づいて復号できるように暗号化して保持し、外部に対して出力できる第 2 の認証データ保持部をさらに含む。

## 【 0 0 3 0 】

請求項 1 8 記載のデータ配信システムは、請求項 1 7 記載のデータ配信システムの構成に加えて、第 1 の認証復号処理部は、公開認証鍵により復号できるように暗号化された第 2 の認証データをさらに復号して出力し、配信制御部は、第 1 の認証復号処理部にて抽出された第 1 の認証データおよび第 2 の認証データに基づいて認証処理を行ない、少なくともコンテンツキーを配信するか否かを判断する。

## 【 0 0 3 1 】

請求項 1 9 記載のデータ配信システムは、請求項 1 5 記載のデータ配信システムの構成に加えて、第 1 のインタフェイス部と第 2 のインタフェイス部とは、携帯電話網により接続される。

## 【 0 0 3 2 】

請求項 2 0 記載のデータ配信システムは、請求項 1 5 記載のデータ配信システムの構成に加えて、第 1 のインタフェイス部は、端末と直接接続可能なコネクタ部を含む。

## 【 0 0 3 3 】

請求項 2 1 記載のデータ配信システムは、請求項 1 6 記載のデータ配信システムの構成に加えて、第 1 のインタフェイス部は、データ格納部と直接接続可能な接続部を含む。

## 【0034】

請求項22記載のデータ配信システムは、請求項21記載のデータ配信システムの構成に加えて、データ解読部は、接続部からのデータを受ける複数の端子を含み、外部からの指令に従って、接続部からデータを受ける端子数が切換え可能である。

## 【0035】

請求項23記載のデータ配信システムは、請求項17記載のデータ配信システムの構成に加えて、データ再生部は、第3の公開暗号鍵にて暗号化されたデータを復号する第3の秘密復号鍵を保持するための第4の鍵保持部と、外部にて第3の公開暗号化鍵によって暗号化された第2の共通鍵を復号し抽出するための第3の復号処理部と、第3の共通鍵を生成する第3のセッションキー発生部と、第3の復号処理部にて復号し抽出した第2の共通鍵に基づいて、第3の共通鍵を暗号化し出力するための第2の暗号化処理部と、外部にて第3の共通鍵に基づいて暗号化されたコンテンツキーを復号し抽出するための第4復号処理部と、記録部に記録された暗号化コンテンツデータを抽出したコンテンツキーにて復号し、再生するためのデータ再生部とをさらに備え、配信データ解読部は、公開認証鍵により復号できるコンテンツ再生部からの与えられる暗号化された第2の認証データを復号して第3の公開鍵を抽出するための第2の認証復号処理部と、第2のセッションキー発生部にて生成した第2の共通鍵を第3の公開暗号化鍵に基づいて暗号化する第3の暗号化処理部と、データ再生部にて第2の共通鍵にて暗号化された第3の共通鍵を受けて、第1の復号処理部にて第2の共通鍵に基づいて復号した第3の共通鍵に基づいて、記録部に格納されたデータを第2の秘密復号鍵にて復号したコンテンツキーを、第1の暗号化処理部にて暗号化し、コンテンツ再生部へ出力を指示する制御部とをさらに備え、制御手段は、第2の認証復号処理部により復号された第2の認証データに基づいて認証処理を行ない、少なくともコンテンツキーを出力するか否かを判断する。

## 【0036】

請求項24記載のデータ配信システムは、請求項16記載のデータ配信システムの構成に加えて、配信データ解読部は、第2の公開鍵によって第2の共通鍵を

暗号化するための第 4 の暗号化処理部をさらに含み、認証復号処理部は、外部から指示される、他の配信データ解読部に少なくともコンテンツキーを移転する移動処理に応じて、他のデータ解読部の公開認証鍵によって復号できる暗号化された第 1 の認証データを、公開認証鍵にて復号して、他のデータ解読部における第 1 の公開暗号化鍵を抽出し、第 2 のセッションキー発生部は、移動処理に応じて、第 2 の共通鍵を発生し、第 3 の暗号化処理部は、移動処理に応じて、他の配信データ解読部の第 1 の公開暗号化鍵に基づいて、第 2 の共通鍵を暗号化し、第 2 の復号処理部は、移動処理に応じて、他の配信データ解読部から第 2 の共通鍵によって暗号化され、入力される第 4 の共通鍵と他の配信データ解読部の第 2 の公開暗号化鍵とを復号して抽出し、第 3 の復号処理部は、移動処理に応じて、第 2 の秘密復号鍵に基づいて、記録部に格納された第 2 の公開暗号化鍵にて暗号化されたデータを復号し、コンテンツキーを抽出し、第 4 の暗号化処理部は、移動処理に応じて、他のメモリカードの第 2 の公開暗号化鍵に基づいて、抽出されたコンテンツキーを暗号化し、第 1 の暗号化処理部は、移動処理に応じて、第 4 の暗号化処理部の出力を第 4 の共通鍵にて暗号化し、他の配信データ解読部に対して出力し、制御手段は、第 2 の認証復号処理部により抽出された他のデータ解読部から出力された第 2 の認証データに基づき認証処理を行ない、少なくともコンテンツキーを出力するか否かを判断する。

## 【 0 0 3 7 】

請求項 2 5 記載のデータ配信システムは、請求項 2 2 記載のデータ配信システムの構成に加えて、配信データ解読部は、認証復号処理は、外部から指示される、他の配信データ解読部から少なくともコンテンツキーを移転する移動受理処理に応じて、第 2 の認証データ保持部が第 2 の認証データを出力し、第 1 の復号処理部は、移動受理処理に応じて、他の配信データ解読部から第 1 の公開暗号化鍵によって暗号化され、入力される他の配信データ解読部にて発生された第 4 の共通鍵を復号して抽出し、第 2 のセッションキー発生部は、移動受理処理に応じて、第 2 の共通鍵を発生し、第 1 の暗号化処理部は、移動受理処理に応じて、第 4 の共通鍵に基づいて、第 2 の公開暗号化鍵と第 2 の共通鍵とを暗号化して出力し、第 2 の復号処理部は、他の配信データ解読部に第 2 の公開暗号化鍵にて暗号化



され、さらに第 2 の共通鍵にて暗号化されたコンテンツキーを第 2 の共通鍵にて復号し、記録部に記録する。

【0038】

請求項 26 記載のデータ配信システムは、請求項 21 記載のデータ配信システムの構成に加えて、コンテンツデータ供給装置は、コンテンツ再生部と共通な第 5 の共通鍵を保持する第 5 の鍵保持部と、第 5 の鍵保持部に保持された第 5 の共通鍵に基づいて、コンテンツキーを暗号化し第 1 のライセンス暗号化処理部に対して出力する第 3 のライセンス暗号化部をさらに含み、コンテンツ再生部は、第 5 の共通鍵を保持する第 6 の鍵保持手段と、第 4 の復号処理部とデータ再生部との間に設けられ、第 6 の鍵保持部に保持された第 5 の共通鍵によって、第 4 の復号処理部の出力からコンテンツキーを復号し抽出し、データ再生部に対して出力する第 5 の復号処理部をさらに含む。

【0039】

請求項 27 記載のデータ配信システムは、請求項 21 記載のデータ配信システムの構成に加えて、コンテンツデータ供給装置は、コンテンツ再生部にて復号可能な第 4 の公開暗号化鍵を保持する第 5 の鍵保持部と、第 4 の公開暗号化鍵に基づいてコンテンツキーを暗号化し第 1 のライセンス暗号化処理部にて出力する第 3 のライセンス暗号化部をさらに含み、コンテンツ再生部は、第 4 の公開暗号化鍵によって暗号化されたデータを復号できる第 4 の秘密復号鍵を保持する第 6 の鍵保持手段と、第 4 の復号処理部とデータ再生部との間に設けられ、第 4 の秘密復号鍵によって第 4 の復号処理部の出力からコンテンツキーを復号し抽出し、データ再生部に対して出力する第 5 の復号処理部をさらに含む。

【0040】

請求項 28 記載のデータ配信システムは、請求項 16 記載のデータ配信システムの構成に加えて、データ再生部は、複数の配信データ解読部を備える。

【0041】

【発明の実施の形態】

ー 【実施の形態 1】

【システムの全体構成】

図1は、本発明の情報配信システムの全体構成を概略的に説明するための概念図である。

【0042】

なお、以下では携帯電話網を介して、音楽データを各ユーザに配信するデータ配信システムの構成を例にとって説明するが、以下の説明で明らかとなるように、本発明はこのような場合に限定されることなく、他の著作物データ、たとえば画像データ等の著作物データを、他の情報通信網を介して配信する場合にも適用することが可能なものである。

【0043】

図1を参照して、著作権の存在する音楽情報を管理する配信サーバ10は、所定の暗号方式により音楽データ（以下コンテンツデータとも呼ぶ）を暗号化したうえで、情報を配信するための配信キャリア20である携帯電話会社に、このような暗号化データを与える。一方、認証サーバ12は、音楽データの配信を求めてアクセスしてきた機器が正規の機器であるか否かの認証を行なう。

【0044】

配信キャリア20は、自己の携帯電話網を通じて、各ユーザからの配信要求（配信リクエスト）を配信サーバ10に中継する。配信サーバ10は、配線リクエストがあると、認証サーバ12により正規の機器からのアクセスであることを確認し、要求されたコンテンツデータをさらに暗号化したうえで、配信キャリア20の携帯電話網を介して、各ユーザの携帯電話機に対して配信する。

【0045】

図1においては、たとえば携帯電話ユーザ1の携帯電話機100には、携帯電話機100により受信された暗号化コンテンツデータを受取って、上記送信にあたって行なわれた暗号化については復号化したうえで、携帯電話機100中の音楽再生部（図示せず）に与えるための着脱可能なメモリカード110に格納する構成となっている。

【0046】

さらに、たとえばユーザ1は、携帯電話機100に接続したヘッドホン130等を介してこのようなコンテンツデータを再生した音楽を聴取することが可能で

ある。

【0047】

以下では、このような配信サーバ10と認証サーバ12と配信キャリア20とを併せて、音楽サーバ30と総称することにする。

【0048】

また、このような音楽サーバ30から、各携帯電話端末等にコンテンツデータを伝送する処理を「配信」と称することとする。

【0049】

このような構成とすることで、まず、正規のメモリカードであるメモリカード110を購入していない正規のユーザでないものは、音楽サーバ30からの配信データを受取って再生することが困難な構成となる。

【0050】

しかも、配信キャリア20において、たとえば1曲分のコンテンツデータを配信するたびにその度数を計数しておくことで、ユーザがコンテンツデータを受信（ダウンロード）するたびに発生する著作権料を、配信キャリア20が携帯電話の通話料金として徴収することとすれば、著作権者が著作権料を確保することが容易となる。

【0051】

しかも、このようなコンテンツデータの配信は、携帯電話網というクローズドなシステムを介して行なわれるため、インターネット等のオープンなシステムに比べて、著作権保護の対策を講じやすいという利点がある。

【0052】

このとき、たとえばメモリカード112を有するユーザ2が、自己の携帯電話機102により、音楽サーバ30から直接コンテンツデータの配信を受けることは可能である。しかしながら、相当量の情報量を有するコンテンツデータ等をユーザ2が直接音楽サーバ30から受信することとすると、その受信のために比較的長い時間を要してしまう場合がある。このような場合、既に当該コンテンツデータの配信を受けているユーザ1から、そのコンテンツデータをコピーできることを可能としておけば、ユーザにとっての利便性が向上する。

【0053】

しかしながら、著作権者の権利保護の観点からは、自由なコンテンツデータのコピーを放任することはシステム構成上許されない。

【0054】

図1に示した例では、ユーザ1が受信したコンテンツデータを、コンテンツデータそのものおよび当該コンテンツデータを再生可能とするために必要な情報とともに、ユーザ2に対してコピーさせる場合をコンテンツデータの「移動」と呼ぶ。この場合、ユーザ1は、再生のために必要な情報（再生情報）ごとユーザ2にコピーさせるため、情報の移動を行なった後には、ユーザ1においてはコンテンツデータの再生を行なうことは不可能とする必要がある。ここで、コンテンツデータは所定の暗号化方式にしたがって暗号化された暗号化コンテンツデータとして配信され、「再生情報」とは、後に説明するように、上記所定の暗号化方式にしたがって暗号化コンテンツデータを復号可能なライセンスキーとも称すると、著作権保護に関わる情報であるライセンスIDデータやユーザIDデータ等のライセンス情報とを意味する。

【0055】

これに対して、コンテンツデータのみを暗号化されたままの状態、ユーザ2にコピーさせることを音楽情報の「複製」と呼ぶこととする。

【0056】

この場合、ユーザ2の端末には、このようなコンテンツデータを再生させるために必要な再生情報はコピーされない、ユーザ2は、暗号化コンテンツデータを得ただけでは、音楽を再生させることができない。したがって、ユーザ2が、このような音楽の再生を望む場合は、改めて音楽サーバ30からコンテンツデータの再生を可能とするための再生情報の配信を受ける必要がある。しかしながら、この場合は、再生を可能とするための情報の配信のみを受ければよい、ユーザ2が直接音楽サーバ30からすべての配信を受ける場合に比べて、格段に短い通話時間で、音楽再生を可能とすることができる。

【0057】

たとえば、携帯電話機100および102が、PHS (Personal Handy Phone

）である場合には、いわゆるトランシーバモードの通話が可能となっているので、このような機能を利用して、ユーザ1からユーザ2への一括した情報の移転（移動）や、暗号化したコンテンツデータのみの転送（複製）を行なうことが可能である。

#### 【0058】

図1に示したような構成においては、暗号化して配信されるコンテンツデータをユーザ側で再生可能とするためにシステム上必要とされるのは、第1には、通信における暗号化キー（鍵）を配送するための方式であり、さらに第2には、配信データを暗号化する方式そのものであり、さらに、第3には、このようにして配信されたデータの無断コピーを防止するためのデータ保護を実現する構成である。

#### 【0059】

##### 〔暗号／復号鍵の構成〕

図2は、図1に示した情報配信システムにおいて使用される通信のためのキーデータ（鍵データ）等の特性をまとめて説明するための図である。

#### 【0060】

まず、図1に示した構成において、メモ리카ード100内のデータ処理を管理するための鍵としては、メモ리카ードという媒体の種類に固有であり、かつ、メモ리카ードの種類等を個別に特定するための情報を含む秘密復号鍵 $K_{media}(n)$ （ $n$ ：自然数）と、メモ리카ードごとに異なる公開暗号化鍵 $K_{Pcard}(n)$ と、公開暗号化鍵 $K_{Pcard}(n)$ により暗号化されたデータを復号するための秘密復号鍵 $K_{card}(n)$ とがある。

#### 【0061】

ここで、鍵 $K_{card}(n)$ や鍵 $K_{Pcard}(n)$ の表記中の自然数 $n$ は、各メモ리카ードを区別するための番号を表わす。

#### 【0062】

すなわち、公開暗号化鍵 $K_{Pcard}(n)$ で暗号化されたデータは、各メモ리카ードごとに存在する秘密復号鍵 $K_{card}(n)$ で復号可能である。したがって、メモ리카ードにおける配信データの授受にあたっては、基本的には、後に

説明するように3つの暗号鍵 $K_{media}(n)$ 、 $K_{card}(n)$ 、 $K_{Pcard}(n)$ が用いられることになる。

【0063】

さらに、メモリカード外とメモリカード間でのデータの授受における秘密保持のための暗号鍵としては、各媒体に固有な公開暗号化鍵 $K_{Pmedia}(n)$ と、公開暗号化鍵 $K_{Pmedia}(n)$ により暗号化されたデータを復号化するための秘密復号鍵 $K_{media}(n)$ と、各通信ごと、たとえば、音楽サーバ30へのユーザのアクセスごとに音楽サーバ30、携帯電話機100または102において生成される共通鍵 $K_s$ が用いられる。

【0064】

ここで、共通鍵 $K_s$ は、たとえば、ユーザが音楽サーバ30に対して1回のアクセスを行なうごとに発生する構成として、1回のアクセスである限り何曲の音楽情報についても同一の共通鍵が用いられる構成としてもよいし、また、たとえば、各曲目ごとにこの共通鍵を変更したうえでその都度ユーザに配信する構成としてもよい。

【0065】

以下では、このような通信の単位あるいはアクセスの単位を「セッション」と呼ぶことにし、共通鍵 $K_s$ を「セッションキー」とも呼ぶことにする。

【0066】

したがって、共通鍵 $K_s$ は各通信セッションに固有の値を有することになり、配信サーバや携帯電話機において管理される。

【0067】

また、配信されるべきデータについては、まず、暗号化コンテンツデータを復号する鍵である $K_c$ （以下、ライセンスキーと呼ぶ）があり、このライセンスキー $K_c$ により暗号化コンテンツデータが復号化されるものとする。さらに、上述したライセンス情報として、当該コンテンツデータを特定できる管理コードや、再生を行なう回数の制限などの情報を含むライセンスIDデータLicense-ID等が存在する。一方、携帯電話は、受信者を識別するためのユーザIDデータUser-IDを保持している。

## 【0068】

このような構成とすることで、ライセンスIDデータに含まれる情報に応じて、著作権者側の著作権保護に関する制御を行なうことが可能であり、一方ユーザIDデータを用いることで、ユーザの個人情報の保護、たとえばユーザのアクセス履歴等が部外者から知ることができないように保護するといったような制御を行なうことが可能である。

## 【0069】

配信データにおけるコンテンツデータDcは、上述のとおり、たとえば音楽データであり、このコンテンツデータをライセンスキーKcで復号化可能なデータを、暗号化コンテンツデータ[Dc]Kcと呼ぶ。

## 【0070】

ここで、[Y]Xという表記は、データYを、キー（鍵）Xにより復号可能な暗号に変換したデータであることを示している。なお、暗号化処理、復号処理で用いられる鍵を、「キー」とも称することとする。

## 【0071】

## 〔配信サーバ10の構成〕

図3は、図1に示した配信サーバ10の構成を示す概略ブロック図である。配信サーバ10は、コンテンツデータ（音楽データ）を所定の方式に従って暗号化したデータや、ライセンスID等の配信情報を保持するための配信情報データベース304と、各ユーザごとにコンテンツデータへのアクセス回数等に従った課金情報を保持するための課金データベース302と、配信情報データベース304および課金データベース302からのデータをデータバスBS1を介して受取り、所定の暗号化処理を行なうためのデータ処理部310と、通信網を介して、配信キャリア20とデータ処理部310との間でデータ授受を行なうための通信装置350とを備える。

## 【0072】

データ処理部310は、データバスBS1上のデータに応じて、データ処理部310の動作を制御するための配信制御部312と、配信制御部312に制御されて、セッションキーKsを発生するためのセッションキー発生部314と、セ

セッションキー発生部 314 より生成されたセッションキー  $K_s$  を、公開暗号化鍵  $KPmedia$  により暗号化して、データバス  $BS1$  に与えるための暗号化処理部 316 と、各ユーザの携帯電話機においてセッションキー  $K_s$  により暗号化されたうえで送信されたデータを通信装置 350 およびデータバス  $BS1$  を介して受けて、復号処理を行なう復号処理部 318 と、復号処理部 318 により抽出された公開暗号化鍵  $KPcard(n)$  を用いて、ライセンスキーやライセンス ID 等のデータを配信制御部 312 に制御されて暗号化するための暗号化処理部 320 と、暗号化処理部 320 の出力を、さらにセッションキー  $K_s$  により暗号化して、データバス  $BS1$  を介して通信装置 350 に与える暗号化処理部 322 とを含む。

## 【0073】

## 〔端末（携帯電話機）の構成〕

図 4 は、図 1 に示した携帯電話機 100 の構成を説明するための概略ブロック図である。

## 【0074】

携帯電話機 100 は、携帯電話網により無線伝送される信号を受信するためのアンテナ 1102 と、アンテナ 1102 からの信号を受けてベースバンド信号に変換し、あるいは携帯電話機からのデータを変調してアンテナ 1102 に与えるための送受信部 1104 と、携帯電話機 100 の各部のデータ授受を行なうためのデータバス  $BS2$  と、データバス  $BS2$  を介して携帯電話機 100 の動作を制御するためのコントローラ 1106 と、受信者を識別するためのユーザ ID データ  $User-ID$  を保持するユーザ ID 保持部 1107 と、外部からの指示を携帯電話機 100 に与えるためのタッチキー部 1108 と、コントローラ 1106 等から出力される情報をユーザに視覚情報として与えるためのディスプレイ 1110 と、通常の通話動作において、データバス  $BS2$  を介して与えられる受信データに基づいて音声を再生するための音声再生部 1112 と、外部との間でデータの授受を行なうためのコネクタ 1120 と、コネクタ 1120 からのデータをデータバス  $BS2$  に与え得る信号に変換し、または、データバス  $BS2$  からのデータをコネクタ 1120 に与え得る信号に変換するための外部インターフェース



部 1122 とを備える。

【0075】

ここで、ユーザ ID データは、たとえばユーザの電話番号等のデータを含む。

携帯電話機 100 は、さらに、音楽サーバ 30 からのコンテンツデータを復号化処理するための着脱可能なメモリカード 110 と、メモリカード 110 とデータバス BS2 との間のデータの授受を制御するためのメモリインタフェース 1200 と、メモリカード 110 と携帯電話機の他の部分とのデータ授受にあたり、データバス BS2 上においてやり取りされるデータを暗号化するためのセッションキー Ks を乱数等により発生するセッションキー発生部 1502 と、セッションキー発生部 1502 により生成されたセッションキーを暗号化して、データバス BS2 に与えるための暗号化処理部 1504 と、セッションキー発生部 1502 において生成された、データバス BS2 上のデータをセッションキー Ks により復号して出力する復号処理部 1506 と、復号処理部 1506 の出力を受けて、音楽信号を再生するための音楽再生部 1508 と、音楽再生部 1508 の出力と音声再生部 1112 の出力とを受けて、動作モードに応じて選択的に出力するための混合部 1510 と、混合部 1510 の出力を受けて、外部に出力するためのアナログ信号に変換するデジタルアナログ変換部 1512 と、デジタルアナログ変換部 1512 の出力を受けて、ヘッドホン 130 と接続するための接続端子 1514 とを含む。

【0076】

なお、説明の簡素化のため本発明のコンテンツデータの配信に関わるブロックのみを記載し、携帯電話機が本来備えている通話機能に関するブロックについては、一部割愛されている。

【0077】

〔メモリカードの構成〕

図 5 は、図 4 に示したメモリカード 110 の構成を説明するための概略ブロック図である。

【0078】

以下では、端末 100 に装着されるメモリカード 110 の公開暗号化鍵 K P m

e d i a と、端末 102 に装着されるメモ리카ード 112 の公開暗号化鍵 K P m e d i a とを区別して、それぞれ、メモ리카ード 110 に対するものを公開暗号化鍵 K P m e d i a (1) と、メモ리카ード 112 に対するものを公開暗号化鍵 K P m e d i a (2) と称することにする。

## 【0079】

また、これに対応して、公開暗号化鍵 K P m e d i a (1) で暗号化されたデータを復号可能であって、これとは非対称な秘密復号鍵を秘密復号鍵 K m e d i a (1) と称し、公開暗号化鍵 K P m e d i a (2) で暗号化されたデータを復号可能であって、これとは非対称な秘密復号鍵を秘密復号鍵 K m e d i a (2) と称することにする。

## 【0080】

このように、媒体固有の公開暗号化鍵を区別することにより、以下の説明で明らかとなるように、メモ리카ードに複数の種類が存在する場合や、より一般的に、メモ리카ード以外の媒体がシステムのオプションとして存在する場合にも、対応することが可能となる。

## 【0081】

メモ리카ード 110 は、メモリインタフェース 1200 との間で信号を端子 1202 を介して授受するデータバス B S 3 と、公開暗号化鍵 K P m e d i a (1) の値を保持し、データバス B S 3 に公開暗号化鍵 K P m e d i a (1) を出力するための K P m e d i a (1) 保持部 1401 と、メモ리카ード 110 に対応する秘密復号鍵 K m e d i a (1) を保持するための K m e d i a (1) 保持部 1402 と、データバス B S 3 にメモリインタフェース 1200 から与えられるデータから、秘密復号鍵 K m e d i a (1) により復号処理をすることにより、セッションキー K s を抽出する復号処理部 1404 と、公開暗号化鍵 K P c a r d (1) を保持するための K P c a r d (1) 保持部 1405 と、復号処理部 1404 により抽出されたセッションキー K s に基づいて、切換スイッチ 1408 からの出力を暗号化してデータバス B S 3 に与えるための暗号化処理部 1406 と、データバス B S 3 上のデータを復号処理部 1404 により抽出されたセッションキー K s により復号処理してデータバス B S 4 に与えるための復号処理部 1

410と、データバスBS4からメモリカードごとに異なる公開暗号化鍵K P c a r d (n)で暗号化されているライセンスキーK c、ライセンスID等のデータを格納し、データバスBS3からライセンスキーK cにより暗号化されている暗号化コンテンツデータ[D c] K cを受けて格納するためのメモリ1412とを備える。

#### 【0082】

切換えスイッチ1408は、接点P a、P b、P cを有し、接点P aにはK P c a r d (1)保持部1405からの公開暗号化鍵K P c a r d (1)が、接点P bにはデータバスBS5が、接点P cには暗号化処理部1414の出力が与えられる。切換えスイッチ1408は、それぞれ、接点P a、P b、P cに与えられる信号を、動作モードが、「配信モード」、「再生モード」、「移動モード」のいずれであるかに応じて、選択的に暗号化処理部1406に与える。

#### 【0083】

メモリカード110は、さらに、秘密復号鍵K c a r d (1)の値を保持するためのK c a r d (1)保持部1415と、公開暗号化鍵K P c a r d (1)により暗号化されており、かつ、メモリ1412から読み出されたライセンスキーK c、ライセンスID等([K c, L i c e n s e] K c a r d (1))を、復号処理してデータバスBS5に与える復号処理部1416と、データの移動処理等において、相手先のメモリカードの公開暗号化鍵K P c a r d (n)を復号処理部1410から受けて、この相手方の公開暗号化鍵K P c a r d (n)に基づいて、データバスBS5上に出力されているライセンスキーK c、ライセンスID等を暗号化したうえで、切換えスイッチ1408に出力するための暗号化処理部1414と、データバスBS3を介して外部とデータの授受を行い、データバスBS5との間でライセンスIDデータ等を受けて、メモリカード110の動作を制御するためのコントローラ1420と、データバスBS5との間でライセンスIDデータ等のデータの授受が可能なレジスタ1500とを備える。

#### 【0084】

なお、図5において実線で囲んだ領域は、メモリカード110内において、外部からの不当な開封処理等が行なわれると、内部データの消去や内部回路の破壊

により、第三者に対してその領域内に存在する回路内のデータ等の読み出しを不能化するためのモジュールTRMに組込まれているものとする。

【0085】

このようなモジュールは、一般にはタンパーレジスタンスモジュール (Tamper Resistance Module) と呼ばれる。

【0086】

もちろん、メモリ1412も含めて、モジュールTRM内に組み込まれる構成としてもよい。しかしながら、図5に示したような構成とすることで、メモリ1412中に保持されているデータは、いずれも暗号化されているデータであるため、第三者はこのメモリ1412中のデータのみでは、音楽を再生することは不可能であり、かつ高価なタンパーレジスタンスモジュール内にメモリ1412を設ける必要がないので、製造コストが低減されるという利点がある。

【0087】

図6および図7は、図1および図3～図5で説明したデータ配信システムにおける配信動作を説明するための第1および第2のフローチャートである。

【0088】

図6および図7においては、ユーザ1が、メモリカード110を用いることで、音楽サーバ30から音楽データの配信を受ける場合の動作を説明している。

【0089】

まず、ユーザ1の携帯電話機100から、ユーザによりタッチキー1108のキーボタンの操作等によって、配信リクエストがなされる (ステップS100)。

【0090】

メモリカード110においては、この配信リクエストに応じて、K P m e d i a (1) 保持部1401から、公開暗号化鍵K P m e d i a (1) を音楽サーバ30に対して送信する (ステップS102)。

【0091】

音楽サーバ30では、メモリカード110から転送された配信リクエストならびに公開暗号化鍵K P m e d i a (1) を受信すると (ステップS104)、受

信した公開暗号化鍵K P m e d i a (1)に基づいて、認証サーバ12に対して照会を行ない、正規メモリカードからのアクセスの場合は次の処理に移行し（ステップS106）、正規メモリカードでない場合には、処理を終了する（ステップS154）。

【0092】

照会の結果、正規メモリカードであることが確認されると、音楽サーバ30では、セッションキー発生部314が、セッションキーK sを生成する。さらに、音楽サーバ30内の暗号化処理部316が、受信した公開暗号化鍵K P m e d i a (1)により、このセッションキーK sを暗号化して暗号化セッションキー[K s] K m e d i a (1)を生成する（ステップS108）。

【0093】

続いて、音楽サーバ30は、暗号化セッションキー[K s] K m e d i a (1)をデータバスB S 1に与える。通信装置350は、暗号化処理部316からの暗号化セッションキー[K s] K m e d i a (1)を、通信網を通じて、携帯電話機100のメモリカード110に対して送信する（ステップS110）。

【0094】

携帯電話機100が、暗号化セッションキー[K s] K m e d i a (1)を受信すると（ステップS112）、メモリカード110においては、メモリインタフェース1200を介して、データバスB S 3に与えられた受信データを、復号処理部1404が、秘密復号鍵K m e d i a (1)により復号処理することにより、セッションキーK sを復号し抽出する（ステップS114）。

【0095】

続いて、配信動作においては、切換スイッチ1408は、接点P aが閉じる状態が選択されているので、暗号化処理部1406は、接点P aを介してK P c a r d (1)保持部1405から与えられる公開暗号化鍵K P c a r d (1)（メモリカード110に対する公開暗号化鍵）を、セッションキーK sにより暗号化し（ステップS116）、データ[K P c a r d (1)] K sを生成する（ステップS118）。

【0096】

携帯電話機100は、暗号化処理部1406により暗号化されたデータ[KPcard(1)]Ksを音楽サーバ30に対して送信する(ステップS120)。

【0097】

音楽サーバ30では、通信装置350によりデータ[KPcard(1)]Ksが受信され(ステップS122)、データバスBS1に与えられたデータ[KPcard(1)]Ksを復号処理部318が、セッションキーKsにより復号処理して、公開暗号化鍵KPcard(1)を復号抽出する(ステップS124)。

【0098】

続いて、配信制御部312は、配信情報データベース304等に保持されているデータを元に、ライセンスIDデータ等を含むライセンス情報データLicenseを生成する(ステップS126)。

【0099】

さらに、音楽サーバ30は、暗号化コンテンツデータ[Dc]Kcを配信情報データベース304より取得して、通信装置350を介して、メモリカード110に送信する(ステップS128)。

【0100】

携帯電話機100がデータ[Dc]Kcを受信すると(ステップS130)、メモリカード110においては、受信したデータ[Dc]Kcをそのままメモリ1412に格納する(ステップS132)。

【0101】

一方、音楽サーバ30は、ライセンスキーKcを配信情報データベース304より取得し(ステップS134)、暗号化処理部320は、配信制御部312からのライセンスキーKcとライセンス情報データLicenseとを、復号処理部318より与えられた公開暗号化鍵KPcard(1)により暗号化処理する(ステップS136)。

【0102】

暗号化処理部322は、暗号化処理部320により暗号化されたデータ[Kc

、License] Kcard (1) を受取って、さらにセッションキーKsにより暗号化したデータをデータバスBS1に与える。通信装置350は、暗号化処理部322により暗号化されたデータ[[Kc, License] Kcard (1)] Ksをメモリカード110に対して送信する。

【0103】

携帯電話機100がデータ[[Kc, License] Kcard (1)] Ksを受信すると(ステップS142)、メモリカード110においては、復号処理部1410がセッションキーKsにより復号処理を行ない、データ[Kc, License] Kcard (1)を抽出し、メモリ1412に記録(格納)する(ステップS146)。

【0104】

さらに、メモリカード110においては、コントローラ1420により制御されて、復号処理部1416が、メモリ1412に格納されたデータ[Kc, License] Kcard (1)を復号し、復号されたライセンス情報データLicenseを、レジスタ1500に格納する(ステップ148)。

【0105】

以上のような動作により、メモリカード自身が、セッションキーKsを送る側(音楽サーバ30)に、公開暗号化鍵KPmedia (1)を送信した上で、配信を受けることができ、メモリカード110が格納するコンテンツデータは再生可能な状態となる。以下では、メモリカードが格納するコンテンツデータが再生可能な状態となっていることを、「メモリカード110は、状態SAにある」と呼ぶことにする。一方、メモリカードが格納するコンテンツデータが再生不可能な状態となっていることを、「メモリカード110は、状態SBにある」と呼ぶことにする。

【0106】

さらに、メモリカード110から音楽サーバ30へは、配信受理が通知され、音楽サーバ30で配信受理を受信すると(ステップS150)、課金データベース302にユーザ1の課金データが格納され(ステップS152)、処理が終了する(ステップS154)。

【0107】

図8は、携帯電話機100内において、メモ리카ード110に保持された暗号化コンテンツデータから、コンテンツデータを復号化し、音楽として外部に出力するための再生処理を説明するフローチャートである。

【0108】

図8を参照して、携帯電話機100のタッチキー部1108等からのユーザ1の指示により、再生リクエストがメモ리카ード110に対して出力される（ステップS200）。

【0109】

メモ리카ード110においては、この再生リクエストに応じて、コントローラ1420は、レジスタ1500に保持されるライセンス情報データLicenseに基づいて、再生可能なデータに対するリクエストであるかを判断し（ステップS202）、再生可能と判断した場合は、KPmedia(1)保持部1401から、公開暗号化鍵KPmedia(1)を携帯電話機100に対して送信する（ステップS204）。一方、再生不可能と判断した場合は、処理を終了する（ステップS230）。

【0110】

再生可能と判断され、メモ리카ード110から公開暗号化鍵KPmedia(1)が送信された場合、携帯電話機100では、メモ리카ード110からの公開暗号化鍵KPmedia(1)を受信すると（ステップS206）、Ks発生部1502においてセッションキーKsを生成し、暗号化処理部1504が、公開暗号化鍵KPmedia(1)により、セッションキーKsを暗号化して暗号化セッションキー[Ks]KPmedia(1)を生成し、データバスBS2を介して、メモ리카ード110に対して送信する（ステップS208）。

【0111】

メモ리카ード110は、データバスBS2を介して、携帯電話機100により生成され、かつ暗号化されたセッションキーKsを受け取り、秘密復号鍵Kmedia(1)により復号し、セッションキーKsを抽出する（ステップS210）。



## 【0112】

続いて、メモリカード110は、メモリ1412から、暗号化されているデータ[Kc, License]Kcard(1)を読み出し、復号処理部1416が復号処理を行なう(ステップS212)。

## 【0113】

秘密復号鍵Kcard(1)により、メモリ1412から読み出されたデータを復号可能な場合(ステップS214)、ライセンスキーKcが抽出される(ステップS216)。一方、再生不可能の場合、処理は終了する(ステップS232)。

## 【0114】

メモリ1412から読み出されたデータを再生可能な場合(ステップS214)は、レジスタ1500内のライセンス情報データLicenseのうち、再生回数に関するデータが変更される(ステップS218)。

## 【0115】

続いて、抽出したセッションキーKsにより、ライセンスキーKcを暗号化し(ステップS220)、暗号化されたライセンスキー[Kc]KsをデータベースBS2に与える(ステップS222)。

## 【0116】

携帯電話機100の復号処理部1506は、セッションキーKsにより復号化処理を行なうことにより、ライセンスキーKcを取得する(ステップS224)。

## 【0117】

続いて、メモリカード110は、暗号化コンテンツデータ[Dc]Kcをメモリ1412から読み出し、データベースBS2に与える(ステップS226)。

## 【0118】

携帯電話機100の音楽再生部1508は、暗号化コンテンツデータ[Dc]Kcを、抽出されたライセンスキーKcにより復号処理して平文の音楽データを生成し(ステップS228)、音楽信号を再生して混合部1510に与える(ステップS230)。デジタルアナログ変換部1512は、混合部1510からの

データを受け取って変換し、外部に再生された音楽を出力し、処理が終了する（ステップS232）。

【0119】

このような構成とすることで、メモリカード自身が、セッションキーKsを送る側（携帯電話機100）に、公開暗号化鍵K<sub>Pmedia</sub>（1）を送信した上で、再生動作を行なうことが可能となる。

【0120】

図9および図10は、2つのメモリカード間において、音楽データおよびキーデータ等の移動または複製を行なう処理を説明するための第1および第2のフローチャートである。

【0121】

まず、携帯電話機102が送信側であり、携帯電話機100が受信側であるものとする。また、携帯電話機102にも、メモリカード110と同様の構成を有するメモリカード112が装着されているものとする。

【0122】

携帯電話機102は、まず、自身の側のメモリカード112および携帯電話機100に対して、移動リクエストまたは複製リクエストを出力する（ステップS300）。

【0123】

メモリカード112は、これに応じて、メモリ1412内の暗号化コンテンツデータ[Dc]Kcを読み出して、メモリカード110に対して出力し（ステップS302）、一方、携帯電話機100は、携帯電話機102からリクエストを受信して（ステップS301）、メモリカード110では、暗号化コンテンツデータ[Dc]Kcをメモリ1412に格納する（ステップS304）。

【0124】

続いて、携帯電話機102および100においては、ステップS300において与えられたリクエストが、「移動リクエスト」であるか「複製リクエスト」であるかが判断され（ステップS306、ステップS306'）、「移動リクエスト」である場合、メモリカード112は、公開暗号化鍵K<sub>Pmedia</sub>（2）を

携帯電話機102に対して送信し（ステップS308）、携帯電話機102は、公開暗号化鍵KPmedia（2）を受信する（ステップS312）。一方、メモリカード110は、「移動リクエスト」である場合、公開暗号化鍵KPmedia（1）を携帯電話機100に出力し（ステップS308'）、携帯電話機100は、公開暗号化鍵KPmedia（1）を携帯電話機102に対して送信する（ステップS310）。

## 【0125】

携帯電話機102が、公開暗号化鍵KPmedia（1）および公開暗号化鍵KPmedia（2）を受信すると（ステップS312、ステップS312'）、携帯電話機102においては、セッションキー発生回路1502は、セッションキーKsを生成し（ステップS303）、公開暗号化鍵KPmedia（1）および公開暗号化鍵KPmedia（2）を用いて、暗号化処理部1504がセッションキーKsを暗号化する（ステップS314）。

## 【0126】

携帯電話機102は、データバスBS2を介して、メモリカード112に対しては暗号化セッションキー[Ks] KPmedia（2）を伝達し、メモリカード112においては、秘密復号鍵Kmedia（2）によりセッションキーKsを復号抽出する（ステップS328）。

## 【0127】

さらに、携帯電話機102は、暗号化セッションキー[Ks] KPmedia（1）を携帯電話機100に対して送信する（ステップS316）。携帯電話機100は、暗号化セッションキー[Ks] KPmedia（1）を受信すると（ステップS318）、メモリカード110に伝達し、メモリカード110は、復号処理部1404が復号して、セッションキーKsを受理する（ステップS320）。

## 【0128】

メモリカード110においては、セッションキーKsによりメモリカード110の公開暗号化鍵KPcard（1）を暗号化して（ステップS322）、携帯電話機100から携帯電話機102に対して暗号化されたデータ[KPcard

(1) ] Ksを送信する(ステップS324)。携帯電話機102は、データ[KPcard(1)] Ksを受信し(ステップS326)、かつ、メモリカード112によるセッションキーKsの受理が完了すると(ステップS328)、メモリカード112においては、メモリカード110から送信された暗号化データ[KPcard(1)] KsをセッションキーKsにより復号化して、メモリカード110の公開暗号化鍵KPcard(1)を復号抽出する(ステップS330)。

【0129】

続いて、メモリカード112においては、メモリ1412からメモリカード112の公開暗号化鍵KPcard(2)により暗号化されているライセンスキーKc、ライセンス情報データLicenseが読み出される(ステップS332)。

【0130】

続いて、メモリカード112の復号処理部1416が、秘密復号鍵Kcard(2)により、ライセンスキーKc、ライセンス情報データLicenseを復号処理する(ステップS334)。

【0131】

メモリカード112のコントローラ1420は、このようにして復号されたライセンス情報データLicenseの値を、レジスタ1500内のデータ値と置換する(ステップS336)。

【0132】

さらに、メモリカード112の暗号化処理部1414は、復号処理部1410において抽出されたメモリカード110における公開暗号化鍵KPcard(1)により、ライセンスキーKc、ライセンス情報データLicenseとを暗号化する(ステップS338)。

【0133】

メモリカード112の暗号化処理部1414により暗号化されたデータは、切換スイッチ1408(接点Pcが閉じている)を介して、さらに、暗号化処理部1406に与えられ、暗号化処理部1406は、データ[Kc, License

] Kcard (1) をセッションキー Ks により暗号化してデータ [[Kc, License] Kcard (1)] Ks を生成する (ステップ S340)。

【0134】

続いて、メモリカード112は、携帯電話機102に対してデータ [[Kc, License] Kcard (1)] Ks を出力し (ステップ S342)、携帯電話機102はデータ [[Kc, License] Kcard (1)] Ks を携帯電話機100に対して送信する (ステップ S344)。

【0135】

携帯電話機100が受信したデータ [[Kc, License] Kcard (1)] Ks は (ステップ S346)、メモリカード110に対して伝達され、メモリカード110の復号処理部1410は、暗号化されたデータ [[Kc, License] Kcard (1)] Ks を復号して、データ [Kc, License] Kcard (1) を受理する (ステップ S348)。

【0136】

メモリカード110においては、復号処理部1410により、セッションキー Ks に基づいて復号化処理されたデータをメモリ1412に記録する (ステップ S350)。さらに、メモリカード110においては、復号処理部1416が、秘密復号鍵 Kcard (1) に基づいて、データ [Kc, License] Kcard (1) を復号し、復号されたライセンス情報データ License をレジスタ1500に格納する (ステップ S352)。

【0137】

復号されたライセンス情報データ License のレジスタ1500への格納が終了すると、メモリカード110は携帯電話機100に移動受理を通知し、携帯電話機100は、携帯電話機102に対して移動受理を送信する (ステップ S354)。

【0138】

携帯電話機102は、携帯電話機100からの移動受理を受信すると、メモリカード112に対してこれを転送し、メモリカード112は、これに応じて、レジスタ1500に格納されたライセンス情報データ License を消去する (

ステップ 358)。

【0139】

一方、携帯電話機 102 では、移動受理が受信されたことに応じて、ディスプレイ 1110 上に、ユーザ 2 に対して、メモリカード 112 のメモリ 1412 内に格納されている移動データに対応する記憶データの消去を行なって良いかを問うメッセージを表示する。これに応じて、ユーザ 2 は、タッチキー 1108 からこのメッセージに対する回答を入力する (ステップ S360)。

【0140】

レジスタ 1500 内のデータの消去が完了し (ステップ S358)、かつ、上記メッセージに対する回答の入力が行なわれると (ステップ S360)、メモリカード 112 内のコントローラ 1420 は、メモリ 1412 内のデータの消去を行なうかの判断を行なう (ステップ S362)。

【0141】

メモリ 1412 内の該当データの消去が指示されている場合 (ステップ S362)、コントローラ 1420 により制御されて、メモリ 1412 内の暗号化コンテンツデータ [Dc] Kc およびデータ [Kc, License] Kcard (2) が消去され (ステップ S364)、処理が終了する (ステップ S374)。

【0142】

一方、メモリ 1412 内の該当データの消去が指示されていない場合 (ステップ S362)、処理は終了する (ステップ S374)。この場合、メモリ 1412 内には、暗号化コンテンツデータ [Dc] Kc およびデータ [Kc, License] Kcard (2) が残っていることになるが、レジスタ 1500 内にライセンス情報データ License が存在しないため、ユーザ 2 は、再度、音楽サーバ 30 から再生情報を配信してもらわない限り、音楽データの再生を行なうことはできない。すなわち、メモリカード 112 は「状態 SB」となる。メモリカード 110 においては、暗号化コンテンツデータ以外にも、ライセンスキー Kc、ライセンス情報データが移動されているので、メモリカード 110 は「状態 SA」となっている。

【0143】

一方、ステップS306'において、「複製リクエスト」が与えられていると判断された場合は、携帯電話機100から携帯電話機102に対して複製受取が送信される（ステップS370）。携帯電話機102において、複製受取を受信すると（ステップS372）、処理が終了する（ステップS374）。

#### 【0144】

このような構成とすることで、メモ리카ード自身が、セッションキーKsを送る側（携帯電話機100）に、公開暗号化鍵K Pmedia（1）およびK Pmedia（2）を送信した上で、移動動作を行なうこと、および複製動作を行なうことが可能となる。

#### 【0145】

##### 【実施の形態2】

実施の形態2のデータ配信システムにおいては、実施の形態1のデータ配信システムの構成と異なって、配信サーバ、携帯電話機およびメモ리카ードの各々が、独自のセッションキーを生成する構成となっていることを1つの特徴とする。すなわち、配信サーバまたは携帯電話機の発生するセッションキーをセッションキーKsとし、一方のメモ리카ード120の発生するセッションキーをセッションキーKs1とし、メモ리카ード120と同様の構成を有する他方のメモ리카ード122の発生するセッションキーをセッションキーKs2とする。

#### 【0146】

すなわち、実施の形態2のデータ配信システムにおいては、システムを構成する機器の各々が、自身でセッションキーを生成し、データを受け取るとき、言い換えるとデータの送信先になっている場合には、相手方（送信元）に対して、まず、セッションキーを配送する。送信元は、この送信先から配送されたセッションキーでデータを暗号化し、この暗号化データを送信する。送信先では、自身で生成したセッションキーにより、受け取ったデータを復号化するという構成を1つの特徴とするものである。

#### 【0147】

また、上記のような動作を実現するために、再生動作において、携帯電話機側がメモ리카ードの生成するセッションキーを受け取るための公開暗号化鍵をK P

pとし、この公開暗号化鍵 $KP_p$ で暗号化されたデータを復号化できる秘密復号鍵を鍵 $K_p$ とする。

#### 【0148】

図11は、実施の形態2のメモリカード120に対応した配信サーバ11の構成を示す概略ブロック図である。図3に示した配信サーバ10の構成と異なる点は、データ処理部310における暗号化処理部322は、 $K_s$ 発生部314からのセッションキー $K_s$ に基づいてではなく、携帯電話機に装着されたメモリカードからセッションキー $K_{s1}$ 、 $K_{s2}$ により暗号化されて送信され、復号処理部318により復号抽出されたセッションキー、たとえば、セッションキー $K_{s1}$ に基づいて、暗号化処理部320の出力をさらに暗号化して、データバス $BS1$ を介して通信装置350に与える点である。

#### 【0149】

配信サーバ11のその他の点は、図3に示した実施の形態1の配信サーバ10の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

#### 【0150】

図12は、実施の形態2における携帯電話機101の構成を説明するための概略ブロック図である。

#### 【0151】

図4に示した携帯電話機100の構成と異なる点は、まず、メモリカード120が装着されていること以外に、携帯電話機101は、公開暗号化鍵 $KP_p$ を保持して、再生動作時に公開暗号化鍵 $KP_p$ をデータバス $BS2$ に出力する $KP_p$ 保持部1524を備える構成となっていることである。

#### 【0152】

さらに、携帯電話機101は、秘密復号鍵 $K_p$ を保持する $K_p$ 保持部1520と、この $K_p$ 保持部1520から与えられる秘密復号鍵 $K_p$ に基づいて、データバス $BS2$ を介してメモリカード120から与えられる公開暗号化鍵 $KP_p$ で暗号化されたセッションキー $K_{s1}$ を復号し抽出する復号処理部1522とをさらに備える構成となっている。しかも、暗号化処理部1504は、この復号処理部



1522から与えられるセッションキーKs1により、Ks発生部1502からの自身のセッションキーKsを暗号化してデータバスBS2に出力する。

【0153】

携帯電話機101のその他の点は、図4に示した実施の形態1の携帯電話機100の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

【0154】

図13は、本発明の実施の形態2のメモリカード120の構成を説明するための概略ブロック図であり、実施の形態1の図5と対比される図である。

【0155】

メモリカード120の構成が、メモリカード110の構成と異なる点は、まず、メモリカード120は、このカード独自のセッションキーKs1を発生するセッションキーKs1発生部1432を備えることである。

【0156】

さらに、メモリカード120は、セッションキー発生回路1432で生成されたセッションキーKs1を、暗号化してデータバスBS3に与えるための暗号化処理部1430を備える。

【0157】

これに応じて、メモリカード120は、さらに、再生モードにおいて、形態電話機101の公開暗号化鍵KPPを受けて保持するKPP受理部1407と、移動モードにおいて、相手方（移動先）の公開暗号化鍵KPmedia(n)を受けて保持するKPmedia受理部1403と、このKPmedia受理部1403の出力とKPP受理部1407の出力とを受けて、動作モードに応じていずれか一方を出力する切換えスイッチ1436を備える。切換えスイッチ1436は、接点PiおよびPhとを有し、接点PiはKPP受理部1407と、接点PhはKPmedia受理部1403とそれぞれ結合する。暗号化処理部1430は、切換えスイッチ1436から与えられる公開暗号化鍵KPmedia(n)または公開暗号化鍵KPPのいずれかにより、Ks1発生部1432からのセッションキーKs1を暗号化して、データバスBS3に与える。

## 【0158】

すなわち、切換えスイッチ1436は、配信動作のとき、および移動動作において移動先となっているときは、未使用状態であり、再生動作の時は、接点P<sub>i</sub>の側に閉じており、移動動作において移動元となっているときは、接点P<sub>h</sub>の側に閉じている。

## 【0159】

メモ리카ード120は、さらに、接点P<sub>e</sub>、P<sub>f</sub>およびP<sub>g</sub>を有し、復号処理部1404から与えられる音楽サーバからのセッションキーK<sub>s</sub>と、K<sub>s</sub>1発生部1432の出力と、データバスBS4から与えられる携帯電話機101からのセッションキーK<sub>s</sub>とを受けて、動作モードに応じていずれか1つを選択的に出力する切換えスイッチ1435を備える。接点P<sub>e</sub>には復号処理部1404からの出力が、接点P<sub>f</sub>にはK<sub>s</sub>1発生部1432の出力が、接点P<sub>g</sub>にはデータバスBS4がそれぞれ結合している。したがって、暗号化処理部1406と復号処理部1410は、この切換えスイッチ1435から与えられるキーに基づいて、それぞれ、暗号化処理および復号処理を行なう。

## 【0160】

すなわち、切換えスイッチ1435は、配信動作の場合に音楽サーバ31からのセッションキーK<sub>s</sub>1の抽出を行なうときは、接点P<sub>e</sub>の側に閉じており、配信動作の場合に音楽サーバ31からの暗号化されたライセンスキーK<sub>c</sub>、ライセンス情報データについてセッションキーK<sub>s</sub>1による復号を行なうときは、接点P<sub>f</sub>の側に閉じている。切換えスイッチ1435は、再生動作において復号処理を行なうときは、接点P<sub>f</sub>の側に閉じており、再生動作において暗号化処理を行なうときは、接点P<sub>g</sub>の側に閉じている。切換えスイッチ1435は、移動動作において移動元となっている場合に復号処理を行なうときは、接点P<sub>f</sub>の側に閉じており、移動動作において移動元となっている場合に暗号化処理を行なうときは、接点P<sub>g</sub>の側に閉じている。切換えスイッチ1435は、移動動作において移動先となっている場合に移動元のセッションキーを受け取るときは、接点P<sub>e</sub>の側に閉じており、移動動作において移動先となっている場合にライセンスキーK<sub>c</sub>およびライセンス情報データLicenseを受け取るときは、接点P<sub>f</sub>の

側に閉じている。

#### 【0161】

メモリカード120は、さらに、接点Pa、Pb、PcおよびPdを有し、Ks1発生部1432から与えられる自身のセッションキーKs1と、KPcard保持部1405の出力と、データバスBS5から与えられるライセンスキーKcと、暗号化処理部1414から与えられ、相手方の公開暗号化鍵KPcard(n)により暗号化されたライセンスキーKcおよびライセンス情報データLicenseを受けて、動作モードに応じていずれか1つを選択的に出力する切換えスイッチ1409を、切換えスイッチ1408の替わりに備える。

#### 【0162】

接点PaにはKs1発生部1432からの出力が、接点PbにはKPcard(1)保持部1405の出力が、接点PcにはデータバスBS5が、接点Pdには暗号化処理部1414の出力が、それぞれ結合している。したがって、暗号化処理部1406は、この切換えスイッチ1409から与えられるデータに対して、それぞれ、暗号化処理を行なう。

#### 【0163】

すなわち、切換えスイッチ1409は、配信モードにおいて、配信先となっている場合に音楽サーバ31に自身の公開暗号化鍵KPcard(1)や自身のセッションキーKs1を送信するときは、順次、接点Pbの側および接点Paの側に閉じる。切換えスイッチ1409は、再生モードのときは、接点Pcの側に閉じており、移動モードにおいて移動元となっているときは、接点Pdの側に閉じている。切換えスイッチ1409は、移動モードにおいて移動先となっている場合にも移動元に自身の公開暗号化鍵KPcard(1)や自身のセッションキーKs1を送信するときは、順次、接点Pbの側および接点Paの側に閉じる。

#### 【0164】

図14および図15は、図13で説明したメモリカード120を用いた配信モードを説明するための第1および第2のフローチャートである。

#### 【0165】

図14および図15においても、ユーザ1が、メモリカード120を用いるこ

とで、音楽サーバ31から音楽データの配信を受ける配信モードの動作を説明している。

【0166】

まず、ユーザ1の携帯電話機101から、ユーザによりタッチキー1108のキーボタンの操作等によって、配信リクエストがなされる（ステップS100）。

【0167】

メモ리카ード120においては、この配信リクエストに応じて、K P m e d i a (1) 保持部1401から、公開暗号化鍵K P m e d i a (1) を音楽サーバ31に対して送信する（ステップS102）。さらに、メモ리카ード120においては、K s 1 発生部1432によりセッションキーK s 1 が生成される（ステップS109）。

【0168】

音楽サーバ31では、メモ리카ード120から転送された配信リクエストならびに公開暗号化鍵K P m e d i a (1) を受信すると（ステップS104）、受信した公開暗号化鍵K P m e d i a (1) に基づいて、認証サーバ12に対して照会を行ない、正規のメモ리카ードを用いたアクセスの場合は次の処理に移行し（ステップS106）、正規のメモ리카ードでない場合には、処理を終了する（ステップS154）。

【0169】

照会の結果、正規のメモ리카ードであることが確認されると、音楽サーバ31では、セッションキー発生部314が、セッションキーK s を生成する。さらに、音楽サーバ31内の暗号化処理部316が、受信した公開暗号化鍵K P m e d i a (1) により、このセッションキーK s を暗号化して暗号化セッションキー[K s] K m e d i a (1) を生成する（ステップS108）。

【0170】

続いて、音楽サーバ31は、暗号化セッションキー[K s] K m e d i a (1) をデータバスB S 1 に与える。通信装置350は、暗号化処理部316からの暗号化セッションキー[K s] K m e d i a (1) を、通信網を通じて、携帯電

話機101のメモリカード120に対して送信する(ステップS110)。

【0171】

携帯電話機101が、暗号化セッションキー[Ks] Kmedia (1)を受信すると(ステップS112)、メモリカード120においては、メモリインタフェース1200を介して、データバスBS3に与えられた受信データを、復号処理部1404が、秘密復号鍵Kmedia (1)で復号処理することにより、セッションキーKsを復号し抽出する(ステップS114)。

【0172】

続いて、配信モードにおいては、切換えスイッチ1409は、接点PaまたはPbが順次閉じる状態が選択されるので、暗号化処理部1406は、接点Paを介してセッションキー発生部1432から与えられるセッションキーKs1と接点Pbを介してKPcard (1)保持部1405から与えられる公開暗号化鍵KPcard (1) (メモリカード120に対する公開暗号化鍵)とを、セッションキーKsにより暗号化し(ステップS116)、データ[KPcard (1)、Ks1] Ksを生成する(ステップS118)。

【0173】

携帯電話機101は、暗号化処理部1406により暗号化されたデータ[KPcard (1)、Ks1] Ksを音楽サーバ31に対して送信する(ステップS120)。

【0174】

音楽サーバ31では、通信装置350によりデータ[KPcard (1)、Ks1] Ksが受信され(ステップS122)、データバスBS1に与えられたデータ[KPcard (1)、Ks1] Ksを復号処理部318が、セッションキーKsにより復号処理して、公開暗号化鍵KPcard (1)およびセッションキーKs1を復号抽出する(ステップS124)。

【0175】

続いて、配信制御部312は、配信情報データベース304等に保持されているデータを元に、ライセンスIDデータ等を含むライセンス情報データLicenseを生成する(ステップS126)。

## 【0176】

さらに、音楽サーバ31は、暗号化コンテンツデータ[Dc]Kcを配信情報データベース304より取得して、通信装置350を介して、メモリカード120に送信する(ステップS128)。

## 【0177】

携帯電話機101が暗号化コンテンツデータ[Dc]Kcを受信すると(ステップS130)、メモリカード120においては、受信した暗号化コンテンツデータ[Dc]Kcをそのままメモリ1412に格納する(ステップS132)。

## 【0178】

一方、音楽サーバ31は、ライセンスキーKcを配信情報データベース304より取得し(ステップS134)、暗号化処理部320は、配信制御部312からのライセンスキーKcとライセンス情報データLicenseとを、復号処理部318より与えられた公開暗号化鍵KCard(1)により暗号化処理する(ステップS136)。

## 【0179】

暗号化処理部322は、暗号化処理部320により暗号化されたデータ[Kc, License]Kcard(1)を受取って、さらに、メモリカード120からのセッションキーKs1により暗号化したデータをデータバスBS1に与える。通信装置350は、暗号化処理部322により暗号化されたデータ[[Kc, License]Kcard(1)]Ks1をメモリカード120に対して送信する。

## 【0180】

携帯電話機101がデータ[[Kc, License]Kcard(1)]Ks1を受信すると(ステップS142)、メモリカード120においては、復号処理部1410が接点Pfを介してKs1発生部1432から与えられるセッションキーKs1により復号処理を行ない、データ[Kc, License]Kcard(1)を抽出し、メモリ1412に格納する(ステップS146)。

## 【0181】

さらに、メモリカード120においては、コントローラ1420により制御さ

れて、復号処理部1416が、メモリ1412に格納されたデータ[Kc, License] Kcard (1)を復号し、復号されたライセンス情報データLicenseを、レジスタ1500に格納する(ステップ148)。

#### 【0182】

以上のような動作により、メモリカード120自身が、暗号化コンテンツデータを送る側(音楽サーバ31)に、公開暗号化鍵KPmedia (1)およびセッションキーKs1を送信した上で、配信を受けることができ、メモリカード120は、音楽情報を再生可能な状態となる。

#### 【0183】

さらに、メモリカード120から音楽サーバ31へは、配信受理が通知され、音楽サーバ31で配信受理を受信すると(ステップS150)、課金データベース302にユーザ1の課金データが格納され(ステップS152)、処理が終了する(ステップS154)。

#### 【0184】

図16および図17は、携帯電話機101内において、メモリカード120に保持された暗号化コンテンツデータから、音楽データであるコンテンツデータを復号化し、音楽として外部に出力するための再生モードを説明する第1および第2のフローチャートである。

#### 【0185】

図16および図17を参照して、携帯電話機のタッチキー1108等からのユーザ1の指示により、再生リクエストがメモリカード120に対して出力される(ステップS200)。

#### 【0186】

メモリカード120においては、この再生リクエストに応じて、コントローラ1420は、レジスタ1500に保持されるライセンス情報データLicenseに基づいて、復号可能なデータに対するリクエストであるかを判断し(ステップS202)、再生可能と判断した場合は、再生可能通知を携帯電話機101に対して送信する(ステップS240)。一方、再生不可能と判断した場合は、処理を終了する(ステップS280)。

## 【0187】

再生可能と判断され、メモリカード120から再生可能通知が送信された場合、携帯電話機101では、公開暗号化鍵K<sub>P</sub>pをメモリカード120に送信し（ステップS242）、K<sub>s</sub>発生部1502においてセッションキーK<sub>s</sub>を生成する（ステップS244）。

## 【0188】

一方、メモリカード120も、セッションキーK<sub>s</sub>1を生成する（ステップS240）。メモリカード120は、さらに、データバスB<sub>S</sub>2を介して携帯電話機101から受けとった公開暗号化鍵K<sub>P</sub>pによりセッションキーK<sub>s</sub>1を暗号化し（ステップS248）、生成された暗号化セッションキー[K<sub>s</sub>1]K<sub>p</sub>を携帯電話機101に対して送信する（ステップS250）。

## 【0189】

携帯電話機101では、メモリカード120からの暗号化セッションキー[K<sub>s</sub>1]K<sub>p</sub>を受信すると、復号処理部1502が、秘密復号鍵K<sub>ap</sub>により復号化してメモリカード120で生成したセッションキーK<sub>s</sub>1を抽出する（ステップS252）。続いて、携帯電話機101の暗号化処理部1504は、携帯電話機101で生成したセッションキーK<sub>s</sub>をセッションキーK<sub>s</sub>1により暗号化して、暗号化セッションキー[K<sub>s</sub>]K<sub>s</sub>1を生成し（ステップS254）、この暗号化セッションキー[K<sub>s</sub>]K<sub>s</sub>1をメモリカード120に対して送信する（ステップS256）。

## 【0190】

メモリカード120は、データバスB<sub>S</sub>2を介して、携帯電話機101により生成された暗号化セッションキー[K<sub>s</sub>]K<sub>s</sub>1を受け取り、セッションキーK<sub>s</sub>1により復号し、携帯電話機101で生成したセッションキーK<sub>s</sub>を抽出する（ステップS258）。

## 【0191】

続いて、メモリカード120は、メモリ1412から、暗号化されているデータ[K<sub>c</sub>, License]K<sub>card</sub>(1)を読み出し、復号処理部1416が復号処理を行なう（ステップS260）。



## 【0192】

秘密復号鍵K c a r d (1)により、メモリ1412から読み出されたデータを復号可能な場合(ステップS262)、ライセンスキーK cが抽出される(ステップS264)。一方、復号不可能の場合、処理は終了する(ステップS280)。

## 【0193】

メモリ1412から読み出されたデータを復号可能な場合は、さらに、レジスタ1500内のライセンス情報データL i c e n s eのうち、再生回数に関するデータが変更される(ステップS266)。

## 【0194】

続いて、メモリカード120においては、暗号化処理部1406が、抽出したセッションキーK sにより、ライセンスキーK cを暗号化し(ステップS268)、暗号化ライセンスキー[K c] K sをデータバスB S 2に与える(ステップS270)。

## 【0195】

携帯電話機101の復号処理部1506は、セッションキーK sにより復号化処理を行なうことにより、ライセンスキーK cを取得する(ステップS272)。

## 【0196】

続いて、メモリカード120は、暗号化コンテンツデータ[D c] K cをメモリ1412から読み出し、データバスB S 2に与える(ステップS274)。

## 【0197】

携帯電話機101の音楽再生部1508は、暗号化コンテンツデータ[D c] K cを、抽出されたライセンスキーK cにより復号処理して平文のコンテンツデータを生成し(ステップS276)、音楽信号を再生して混合部1510に与える(ステップS276)。デジタルアナログ変換部1512は、混合部1510からの音楽信号を受け取って変換し、外部に再生された音楽を出力し、処理が終了する(ステップS232)。

## 【0198】

このような構成とすることで、メモ리카ード自身および携帯電話自身が、それぞれセッションキー $Ks1$ または $Ks$ を生成し、これにより暗号化されたデータの授受を行なった上で、再生動作を行なうことが可能となる。

#### 【0199】

図18および図19は、2つのメモ리카ード間において、コンテンツデータおよびキーデータ等の移動モードまたは複製モードを行なう処理を説明するための第1および第2のフローチャートである。

#### 【0200】

まず、携帯電話機101と同様の構成を有する携帯電話機103が送信側であり、携帯電話機101が受信側であるものとする。また、携帯電話機103にも、メモ리카ード120と同様の構成を有するメモ리카ード122が装着されているものとする。

#### 【0201】

携帯電話機103は、まず、自身の側のメモ리카ード122および携帯電話機101に対して、移動リクエストまたは複製リクエストを出力する（ステップS300）。

#### 【0202】

メモ리카ード122は、これに応じて、メモリ1412内の暗号化コンテンツデータ[Dc]Kcを読み出して、メモ리카ード120に対して出力し（ステップS302）、一方、携帯電話機101は、携帯電話機103からのリクエストを受信し（ステップS301）、メモ리카ード120では、暗号化コンテンツデータ[Dc]Kcをメモリ1412に格納する（ステップS304）。

#### 【0203】

続いて、携帯電話機103および101においては、ステップS300において与えられたリクエストが、「移動リクエスト」であるか「複製リクエスト」であるかが判断され（ステップS306、ステップS306'）、「移動リクエスト」である場合、メモ리카ード120は、公開暗号化鍵 $KPmedia(1)$ を携帯電話機101に出力し（ステップS308）、携帯電話機101は、公開暗号化鍵 $KPmedia(1)$ を携帯電話機103に対して送信する（ステップS

310)。

【0204】

携帯電話機103が、公開暗号化鍵 $KPmedia(1)$ を受信し(ステップS312)、メモリカード122に転送すると(ステップS313)、メモリカード122の $Ks2$ 発生回路1432は、セッションキー $Ks2$ を生成し(ステップS314)、公開暗号化鍵 $KPmedia(1)$ を用いて、暗号化処理部1430がセッションキー $Ks2$ を暗号化する(ステップS315)。

【0205】

携帯電話機103は、暗号化セッションキー $[Ks2] KPmedia(1)$ を携帯電話機101に対して送信する(ステップS316)。携帯電話機101は、暗号化セッションキー $[Ks2] KPmedia(1)$ を受信すると(ステップS318)、メモリカード120に伝達し、メモリカード120は、復号処理部1404が復号して、セッションキー $Ks2$ を受理し、さらに、セッションキー生成部1432で、メモリカード120におけるセッションキー $Ks1$ が生成される(ステップS320)。

【0206】

メモリカード120においては、セッションキー $Ks2$ によりメモリカード120の公開暗号化鍵 $KPcard(1)$ およびセッションキー $Ks1$ を暗号化して(ステップS322)、携帯電話機101から携帯電話機103に対して暗号化されたデータ $[KPcard(1), Ks1] Ks2$ を送信する(ステップS324)。携帯電話機103は、データ $[KPcard(1), Ks1] Ks2$ を受信し(ステップS326)、メモリカード122に転送する。

【0207】

メモリカード122においては、復号処理部1410が、メモリカード120から送信された暗号化データ $[KPcard(1), Ks1] Ks2$ をセッションキー $Ks2$ により復号化して、メモリカード120の公開暗号化鍵 $KPcard(1)$ 、セッションキー $Ks1$ を復号抽出する(ステップS330)。

【0208】

続いて、メモリカード122においては、メモリ1412からメモリカード1

22の公開暗号化鍵K P c a r d (2)により暗号化されているライセンスキーK c、ライセンス情報データL i c e n s eに対応する[K c、L i c e n s e] K c a r d (2)が読み出される(ステップS332)。

【0209】

続いて、メモリカード122の復号処理部1416が、秘密復号鍵K c a r d (2)により、[K c、L i c e n s e] K c a r d (2)を復号処理する(ステップS334)。

【0210】

メモリカード122のコントローラ1420は、このようにして復号されたライセンス情報データL i c e n s eの値を、レジスタ1500内のデータ値と置換する(ステップS336)。

【0211】

さらに、メモリカード122の暗号化処理部1414は、復号処理部1410において抽出されたメモリカード120における公開暗号化鍵K P c a r d (1)により、ライセンスキーK c、ライセンス情報データL i c e n s eとを暗号化する(ステップS338)。

【0212】

メモリカード122の暗号化処理部1414により暗号化されたデータは、切換えスイッチ1409(接点P dが閉じている)を介して、さらに、暗号化処理部1406に与えられ、メモリカード122の暗号化処理部1406は、データ[K c、L i c e n s e] K c a r d (1)をセッションキーK s 1により暗号化してデータ[[K c、L i c e n s e] K c a r d (1)] K s 1を生成する(ステップS340)。

【0213】

続いて、メモリカード122は、携帯電話機103に対してデータ[[K c、L i c e n s e] K c a r d (1)] K s 1を出力し(ステップS342)、携帯電話機103はデータ[[K c、L i c e n s e] K c a r d (1)] K s 1を携帯電話機101に対して送信する(ステップS344)。

【0214】

携帯電話機101が受信したデータ[[Kc, License] Kcard (1)] Ks1は(ステップS346)、メモリカード120に対して伝達され、メモリカード120の復号処理部1410は、暗号化されたデータ[[Kc, License] Kcard (1)] Ks1を復号して、データ[Kc, License] Kcard (1)を受理する(ステップS348)。

#### 【0215】

メモリカード120においては、復号処理部1410により、セッションキーKs1に基づいて復号化処理されたデータ[Kc, License] Kcard (1)をメモリ1412に格納する(ステップS350)。さらに、メモリカード120においては、復号処理部1416が、秘密復号鍵Kcard (1)に基づいて、データ[Kc, License] Kcard (1)を復号し、復号されたライセンス情報データLicenseをレジスタ1500に格納する(ステップS352)。

#### 【0216】

以後の移動モードにおける処理ならびに複製モードにおけるメモリカード120および122の処理は、図9および図10で説明した実施の形態1のメモリカード110、112等の処理と同様であるので、その説明は繰り返さない。

#### 【0217】

このような構成とすることで、移動元および移動先のメモリカード自身が、セッションキーをそれぞれ生成した上で、移動モードを行なうが可能となる。

#### 【0218】

したがって、データバス上等で伝達されるデータのライセンスキーKcおよびライセンス情報データLicenseを暗号化する鍵が、セッションごとに、かつ、機器ごとに変更されるので、ライセンスキーKcおよびライセンス情報データLicenseの授受のセキュリティが一層向上するという効果がある。

#### 【0219】

しかも、以上のような構成を用いることで、たとえば、メモリカード122からメモリカード120へのデータの移動を、上述したようなセッションキー発生回路1502を有する携帯電話端末を介さずに、メモリカードとメモリカードと

を接続可能なインターフェース機器により行なうことも可能となり、ユーザの利便性が一層向上するという効果がある。

#### 【0220】

ここで、移動時には、再生回数を制限するライセンス情報データ内の設定については、メモリ1412に記録されたライセンス情報データを、レジスタ1500にて再生の都度修正された再生回数を記録したライセンス情報データに変更することで、ライセンス情報データを更新する。このようにして、メモリカード間をコンテンツデータが移動しても、再生回数に制限があるコンテンツデータの再生回数は、配信時に決められた再生回数の制限を越えることがないようにすることが可能である。

#### 【0221】

##### 〔実施の形態3〕

実施の形態3のデータ配信システムにおいては、ユーザは、配信キャリアである携帯電話会社から暗号化コンテンツデータの配信を受けるのではなく、たとえば、街頭などに設置されているコンテンツデータ販売機から暗号化コンテンツデータの供給を受ける構成となっていることを1つの特徴とする。

#### 【0222】

図20は、このような実施の形態3のデータ配信システムの構成を説明するための概念図である。なお、携帯電話機100およびメモリカード110の構成は実施の形態1で説明したものと同様であるので、その説明は繰り返さない。

#### 【0223】

図20を参照して、コンテンツデータ販売機2000は、ユーザに対して配信作業における案内等を出力するためのディスプレイ2002と、ユーザから指示を入力するためのキーボード2004と、料金投入口2006と、携帯電話機100とコネクタ1120を介してデータの授受を行なうための外部コネクタ2010とを備える。さらに、コンテンツデータ販売機2000は、携帯電話網等の通信路を介して、販売記録等を管理するための管理サーバ2200と接続している。

#### 【0224】

図21は、実施の形態3のコンテンツデータ販売機2000の構成を示す概略ブロック図である。コンテンツデータ販売機2000は、上述したように、ディスプレイ2002と、キーボード2004と、料金投入口2006からの投入金を受ける料金受理部2020と、外部コネクタ2010と、コネクタ2010とデータバスとの間に設けられるインターフェース部2012と、コンテンツデータ（音楽データ）を所定の方式に従って暗号化したデータや、ライセンス情報データ等の配信情報を保持するための配信情報データベース304と、管理サーバ2200との間で情報の授受をするための通信装置360と、配信情報データベース304および管理サーバ2200からのデータをデータバスBS1を介して受取り、所定の暗号化処理を行なうためのデータ処理部2100とを備える。

#### 【0225】

データ処理部2100中は、実施の形態1と同様に、データバスBS1上のデータに応じて、データ処理部2100の動作を制御するための配信制御部312と、配信制御部312に制御されて、セッションキーKsを発生するためのセッションキー発生部314と、セッションキー発生部314より生成されたセッションキーKsを、カード媒体に固有な公開暗号化鍵KPmedia(n)により暗号化して、データバスBS1に与えるための暗号化処理部316と、各ユーザの携帯電話機においてセッションキーKsにより暗号化されたうえでコネクタ2010から与えられたデータをデータバスBS1を介して受けて、復号処理を行なう復号処理部318と、復号処理部318により抽出された公開暗号化鍵KPcard(n)を用いて、ライセンス情報データを配信制御部312に制御されて暗号化するための暗号化処理部320と、暗号化処理部320の出力を、さらにセッションキーKsにより暗号化して、データバスBS1を介してコネクタ2010に与える暗号化処理部322とを含む。

#### 【0226】

図22および図23は、図20および図21で説明したデータ配信システムにおける配信モードを説明するための第1および第2のフローチャートである。

#### 【0227】

図22および図23においては、ユーザ1が、メモリカード110を用いるこ

とで、コンテンツデータ販売機2000から音楽データの配信を受ける場合の動作を説明している。

【0228】

まず、ユーザが、コンテンツデータ販売機2000のキーボード2004のキーボタンの操作等によって、配信リクエストを指示する（ステップS400）。コンテンツデータ販売機2000は、メモリカード110に対して公開暗号化鍵KPmedia(1)の送信依頼を出力する（ステップS402）。

【0229】

メモリカード110においては、この公開暗号化鍵KPmedia(1)の送信依頼に応じて、KPmedia(1)保持部1401から、公開暗号化鍵KPmedia(1)を携帯電話機100に対して出力する（ステップS406）。

【0230】

携帯電話機100がコンテンツデータ販売機2000に公開暗号化鍵KPmedia(1)を送信し（ステップS408）、コンテンツデータ販売機2000が、メモリカード110から転送された公開暗号化鍵KPmedia(1)を受信すると（ステップS410）、ディスプレイ2002を介してユーザに料金投入を案内し、料金徴収を行なう（ステップS412）。続いて、コンテンツデータ販売機2000は、セッションキー発生部314が、セッションキーKsを生成する。さらに、コンテンツデータ販売機2000内の暗号化処理部316が、受信した公開暗号化鍵KPmedia(1)により、このセッションキーKsを暗号化して暗号化セッションキー[Ks]Kmedia(1)を生成する（ステップS414）。

【0231】

続いて、コンテンツデータ販売機2000は、暗号化セッションキー[Ks]Kmedia(1)をデータベースBS1に与え、コネクタ2010から出力する（ステップS416）。携帯電話機100は、この暗号化セッションキー[Ks]Kmedia(1)を受信すると、メモリカード110に転送する（ステップS418）。

【0232】



メモ리카ード110においては、メモリインタフェース1200を介して、データバスBS3に与えられた暗号化セッションキー[Ks] Kmedia (1)を、復号処理部1404が、秘密復号鍵Kmedia (1)により復号処理することにより、セッションキーKsを復号し抽出する(ステップS420)。

【0233】

続いて、配信モードにおいては、切換えスイッチ1408は、接点Paが閉じる状態が選択されているので、暗号化処理部1406は、接点Paを介してKPcard (1) 保持部1405から与えられる公開暗号化鍵KPcard (1)を、セッションキーKsにより暗号化し(ステップS422)、データ[KPcard (1)] Ksを生成する(ステップS424)。

【0234】

携帯電話機100は、暗号化処理部1406により暗号化されたデータ[KPcard (1)] Ksをコンテンツデータ販売機2000に対して送信する(ステップS426)。

【0235】

コンテンツデータ販売機2000では、コネクタ2010を介してデータ[KPcard (1)] Ksが受信され(ステップS428)、データバスBS1に与えられたデータ[KPcard (1)] Ksを復号処理部318が、セッションキーKsにより復号処理して、公開暗号鍵KPcard (1)を復号抽出する(ステップS430)。

【0236】

続いて、配信制御部312は、配信情報データベース304等に保持されているデータを元に、ライセンスIDデータ等を含むライセンス情報データLicenseを生成する(ステップS432)。

【0237】

さらに、コンテンツデータ販売機2000は、暗号化コンテンツデータ[Dc] Kcを配信情報データベース304より取得して、コネクタ2010を介して、携帯電話機100に送信する(ステップS434)。

【0238】

携帯電話機 100 が暗号化コンテンツデータ [Dc] Kc を受信すると（ステップ S436）、メモリカード 110 においては、受信した暗号コンテンツデータ [Dc] Kc をそのままメモリ 1412 に格納する（ステップ S438）。

【0239】

一方、コンテンツデータ販売機 2000 は、ライセンスキー Kc を配信情報データベース 304 より取得し（ステップ S440）、暗号化処理部 320 は、配信制御部 312 からのライセンスキー Kc とライセンス情報データ License とを、復号処理部 318 より与えられた公開暗号化鍵 KPcard (1) により暗号化処理する（ステップ S442）。

【0240】

暗号化処理部 322 は、暗号化処理部 320 により暗号化されたデータ [Kc, License] Kcard (1) を受取って、さらにセッションキー Ks により暗号化したデータをデータバス BS1 に与え、暗号化処理部 322 により暗号化されたデータ [[Kc, License] Kcard (1)] Ks がメモリカード 110 に対して送信される（ステップ S446）。

【0241】

携帯電話機 100 がデータ [[Kc, License] Kcard (1)] Ks を受信すると（ステップ S448）、メモリカード 110 においては、復号処理部 1410 がセッションキー Ks により復号処理を行ない、データ [Kc, License] Kcard (1) を抽出し、メモリ 1412 に格納する（ステップ S452）。

【0242】

さらに、メモリカード 110 においては、コントローラ 1420 により制御されて、復号処理部 1416 が、メモリ 1412 に格納されたデータ [Kc, License] Kcard (1) を復号し、復号されたライセンス情報データ License を、レジスタ 1500 に格納する（ステップ S458）。

【0243】

以上のような動作により、メモリカード自身が、セッションキー Ks を送る側（コンテンツデータ販売機 2000）に、公開暗号化鍵 KPmedia (1) を

送信した上で、配信を受けることができ、メモ리카ード110に格納された暗号化コンテンツデータを用いて音楽を再生可能な状態となる。

#### 【0244】

さらに、メモ리카ード110からコンテンツデータ販売機2000へは、携帯電話機100を介して配信受理が通知され（ステップS460）、コンテンツデータ販売機2000で配信受理を受信すると（ステップS462）、管理サーバに販売記録が送信され（ステップS464）、処理が終了する（ステップS466）。

#### 【0245】

以上のような構成により、ユーザは、より簡易に暗号化された音楽データ等の配信を受けることができる。

#### 【0246】

##### 【実施の形態3の変形例】

実施の形態3のデータ配信システムにおいては、メモ리카ード110は、携帯電話機100を介して、コンテンツデータ販売機2000から暗号化コンテンツデータの配信を受ける構成であった。

#### 【0247】

しかしながら、図21に示したコンテンツデータ販売機2000の構成において、コネクタ2010の代わりに、メモ리카ード110との間のインターフェースのためのメモリスロットを設ける構成とすれば、携帯電話機100を介することなく、メモ리카ード110とコンテンツデータ販売機2000とが直接データの授受を行なうことが可能である。

#### 【0248】

図24は、このような実施の形態3の変形例のコンテンツデータ販売機2001の構成を示す概念図である。図20に示した実施の形態3のコンテンツデータ販売機2000の構成と異なる点は、外部コネクタ2010の代わりに、メモ리카ードを挿入できるカードスロット2030が設けられ、このカードスロット2030がインターフェース部2012を介して、データバスBS1とデータの授受をする構成となっている点である。

## 【0 2 4 9】

図 2 5 および図 2 6 は、実施の形態 3 の変形例のデータ配信システムにおける配信モードを説明するための第 1 および第 2 のフローチャートである。

## 【0 2 5 0】

図 2 2 および図 2 3 に示した実施の形態 3 の配信モードとは、携帯電話機 1 0 0 を介さずに、メモリカード 1 1 0 とコンテンツデータ販売機 2 0 0 1 がデータの授受をする点を除いては、同様の処理であるので、同一処理には同一符号を付して、その説明は繰り返さない。

## 【0 2 5 1】

以上のような構成および動作により、一層簡易に、ユーザは暗号化された音楽データ等の配信を受けることができる。

## 【0 2 5 2】

しかも、メモリカードが独立して、暗号化コンテンツデータの配信を受け、格納できるので、コンテンツデータの再生を行なう手段の選択の幅が広がり、よりユーザの利便性が向上するという利点もある。

## 【0 2 5 3】

## 〔実施の形態 4〕

図 2 7 は、実施の形態 4 のコンテンツデータ販売機 3 0 0 0 の構成を説明するための概略ブロック図である。図 2 1 に示したコンテンツデータ販売機 2 0 0 0 の構成と異なる点は、対象となるメモリカードが実施の形態 2 のメモリカード 1 2 0 であり、かつ使用される端末が携帯電話機 1 0 1 である点、およびこれに対応して、データ処理部 2 1 0 0 における暗号化処理部 3 2 2 は、K s 発生部 3 1 4 からのセッションキー K s に基づいてではなく、携帯電話機に装着されたメモリカードからセッションキー K s により暗号化されて送信され、復号処理部 3 1 8 により復号抽出されたセッションキー、たとえば、セッションキー K s 1 に基づいて、暗号化処理部 3 2 0 の出力をさらに暗号化して、データバス B S 1 を介してインターフェース部 2 0 1 2 およびコネクタ 2 0 1 0 に与える点である。

## 【0 2 5 4】

コンテンツデータ販売機 3 0 0 0 のその他の点は、図 2 1 に示した実施の形態

3のコンテンツデータ販売機2000の構成の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

【0255】

また、携帯電話機101およびメモリカード110の構成も実施の形態2で説明したものと同様であるので、その説明も繰り返さない。

【0256】

図28および図29は、図27で説明したデータ配信システムにおける配信モードを説明するための第1および第2のフローチャートである。

【0257】

図28および図29においては、ユーザ1が、メモリカード120を用いることで、コンテンツデータ販売機3000から音楽データの配信を受ける場合の動作を説明している。

【0258】

まず、ユーザが、コンテンツデータ販売機3000のキーボード2004のキーボタンの操作等によって、配信リクエストを指示する（ステップS500）。コンテンツデータ販売機3000は、メモリカード110に対して公開暗号化鍵KPmedia(1)の送信依頼を出力する（ステップS502）。

【0259】

メモリカード120においては、この公開暗号化鍵KPmedia(1)の送信依頼に応じて、KPmedia(1)保持部1401から、公開暗号化鍵KPmedia(1)をコンテンツデータ販売機3000に対して送信する（ステップS506）。さらに、メモリカード120においては、Ks1発生部1432によりセッションキーKs1が生成される（ステップS515）。

【0260】

携帯電話機101がコンテンツデータ販売機3000に公開暗号化鍵KPmedia(1)を送信し（ステップS508）、コンテンツデータ販売機3000が、メモリカード120から転送された公開暗号化鍵KPmedia(1)を受信すると（ステップS510）、ディスプレイ2002を介してユーザに料金投入を案内し、料金徴収を行なう（ステップS512）。続いて、コンテンツデー

タ販売機3000は、セッションキー発生部314が、セッションキーKsを生成する。さらに、コンテンツデータ販売機3000内の暗号化処理部316が、受信した公開暗号化鍵K P m e d i a (1)により、このセッションキーKsを暗号化して暗号化セッションキー [Ks] K m e d i a (1) を生成する（ステップS514）。

## 【0261】

続いて、コンテンツデータ販売機3000は、暗号化セッションキー [Ks] K m e d i a (1) をデータバスBS1に与え、コネクタ2010から出力する（ステップS416）。携帯電話機101は、この暗号化セッションキー [Ks] K m e d i a (1) を受信すると、メモ리카ード120に転送する（ステップS518）。

## 【0262】

メモ리카ード120においては、メモリインタフェース1200を介して、データバスBS3に与えられた暗号化セッションキー [Ks] K m e d i a (1) を、復号処理部1404が、秘密復号鍵K m e d i a (1) により復号処理することにより、セッションキーKsを復号し抽出する（ステップS520）。

## 【0263】

続いて、暗号化処理部1406は、K P c a r d (1) 保持部1405から与えられる公開暗号化鍵K P c a r d (1) およびKs1発生部1432からのセッションキーKs1を、セッションキーKsにより暗号化し（ステップS522）、データ [K P c a r d (1)、Ks1] Ksを生成する（ステップS524）。

## 【0264】

携帯電話機101は、暗号化処理部1406により暗号化されたデータ [K P c a r d (1)、Ks1] Ksをコンテンツデータ販売機3000に対して送信する（ステップS526）。

## 【0265】

コンテンツデータ販売機3000では、コネクタ2010を介してデータ [K P c a r d (1)、Ks1] Ksが受信され（ステップS528）、データバス

BS1に与えられたデータ[KPcard(1)、Ks1]Ksを復号処理部318が、セッションキーKsにより復号処理して、公開暗号化鍵KPcard(1)およびセッションキーKs1を復号抽出する(ステップS530)。

【0266】

続いて、配信制御部312は、配信情報データベース304等に保持されているデータを元に、ライセンスIDデータ等を含むライセンス情報データLicenseを生成する(ステップS532)。

【0267】

さらに、コンテンツデータ販売機3000は、暗号化コンテンツデータ[Dc]Kcを配信情報データベース304より取得して、コネクタ2010を介して、携帯電話機101に送信する(ステップS534)。

【0268】

携帯電話機101が暗号化コンテンツデータ[Dc]Kcを受信すると(ステップS536)、メモリカード120においては、受信した暗号化コンテンツデータ[Dc]Kcをそのままメモリ1412に格納する(ステップS538)。

【0269】

一方、コンテンツデータ販売機3000は、ライセンスキーKcを配信情報データベース304より取得し(ステップS540)、暗号化処理部320は、配信制御部312からのライセンスキーKcとライセンス情報データLicenseとを、復号処理部318より与えられた公開暗号化鍵KPcard(1)により暗号化処理する(ステップS542)。

【0270】

暗号化処理部322は、暗号化処理部320により暗号化されたデータ[Kc、License]Kcard(1)を受取って、さらにセッションキーKs1により暗号化したデータをデータバスBS1に与え、暗号化処理部322により暗号化されたデータ[[Kc、License]Kcard(1)]Ks1が携帯電話機101に対して出力される(ステップS546)。

【0271】

携帯電話機101がデータ[[Kc、License]Kcard(1)]K

s 1を受信すると（ステップS548）、メモリカード120においては、復号処理部1410がセッションキーKs1により復号処理を行ない、データ[Kc, License]Kcard(1)を抽出し、メモリ1412に格納する（ステップS552）。

#### 【0272】

以下の処理は、図22および図23に示した実施の形態3の処理と同様であるので、その説明は繰り返さない。

#### 【0273】

以上のような構成により、ユーザは、より簡易に暗号化された音楽データ等のコンテンツデータ配信を受けることができる。

#### 【0274】

しかも、データバス上で伝達されるデータの暗号化キーが、セッションごとに、かつ、機器ごとに変更されるので、データ授受のセキュリティが一層向上するという効果がある。

#### 【0275】

##### 〔実施の形態4の変形例〕

実施の形態4のデータ配信システムにおいては、メモリカード120は、携帯電話機101を介して、コンテンツデータ販売機3000から暗号化コンテンツデータの配信を受ける構成であった。

#### 【0276】

しかしながら、図27に示したコンテンツデータ販売機3000の構成において、実施の形態3の変形例と同様に、コネクタ2010の代わりに、メモリカード120との間のインターフェースのためにメモリスロットを設ける構成とすれば、携帯電話機101を介することなく、メモリカード120とコンテンツデータ販売機3000とが直接データの授受を行なうことが可能である。

#### 【0277】

このような実施の形態4の変形例のコンテンツデータ販売機3001の構成は、データ処理部2100の構成を除いて、図24に示した実施の形態3の変形例の構成と同様である。



## 【0278】

すなわち、実施の形態4の変形例のコンテンツデータ販売機3001の構成は、図27に示した実施の形態4のコンテンツデータ販売機3000の構成と異なり、外部コネクタ2010の代わりに、メモ리카ードを挿入できるカードスロット2030が設けられ、このカードスロット2030がインターフェース部2012を介して、データバスBS1とデータの授受をする構成となっている。

## 【0279】

図30および図31は、実施の形態4の変形例のデータ配信システムにおける配信モードを説明するための第1および第2のフローチャートである。

## 【0280】

図28および図29に示した実施の形態3の配信モードとは、携帯電話機101を介さずに、メモ리카ード120とコンテンツデータ販売機3001がデータの授受をする点を除いては、同様の処理であるので、同一処理には同一符号を付して、その説明は繰り返さない。

## 【0281】

以上のような構成および動作により、一層簡易に、ユーザは暗号化された音楽データ等の配信を受けることができる。

## 【0282】

しかも、メモ리카ードが独立して、暗号化コンテンツデータの配信を受け、格納できるので、音楽の再生を行なう手段の選択の幅が広がり、よりユーザの利便性が向上するという利点もある。

## 【0283】

## 〔実施の形態5〕

実施の形態5の配信サーバ12、携帯電話機105およびメモ리카ード140は、以下に説明するように、実施の形態2の配信サーバ11、携帯電話機101およびメモ리카ード120の構成とは、以下の点で異なることを特徴とする。

## 【0284】

すなわち、実施の形態5の携帯電話機105では、たとえば、あらかじめ配信システムにおける認証機構等の管理部門にこの携帯電話機105を登録する際に

、この携帯電話機 105 に割当てられた公開暗号鍵 K P p および証明データ C r t f とを公開復号鍵（公開認証鍵）K P m a s t e r により暗号化された形で記録保持する手段を有している。

【0285】

同様に、実施の形態 5 のメモリカード 140 でも、たとえば、あらかじめ配信システムにおける認証機構等の管理部門にこのメモリカード 140 を登録する際に、このメモリカードに割当てられた公開暗号鍵 K P m e d i a および証明データ C r t f とを公開復号鍵（公開認証鍵）K P m a s t e r により暗号化された形で記録保持する手段を有している。

【0286】

ここで、メモリカード 140 および実施の形態 5 の配信サーバ 12 には、この公開復号鍵（公開認証鍵）K P m a s t e r を記録保持する手段を有している。この公開復号鍵（公開認証鍵）K P m a s t e r は、システム中でデータ出力を行なう全ての機器がセッションキーのやりとりに対して、相互にデータの授受を行なえる機器であることの証明と、セッションキーを相手方に送付する際に用いる暗号化鍵の獲得に用いるシステム共通の復号鍵である。

【0287】

以下、さらに、実施の形態 5 の携帯電話機 105、メモリカード 140 および配信サーバ 12 の構成をより詳しく説明する。

【0288】

図 32 は、実施の形態 5 における携帯電話機 105 の構成を説明するための概略ブロック図である。

【0289】

図 12 に示した実施の形態 2 の携帯電話機 101 の構成と異なる点は、K P p 保持部 1524 の替わりに、公開復号鍵（公開認証鍵）K P m a s t e r により暗号化された、公開暗号鍵 K P p および証明データ C r t f を保持するための [ K P p , C r t f ] K P m a s t e r 保持部 1525 を備える構成となっていることである。

【0290】

携帯電話機 105 のその他の点は、図 12 に示した実施の形態 2 の携帯電話機 101 の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

【0291】

図 33 は、実施の形態 5 のメモリカード 140 に対応した配信サーバ 12 の構成を示す概略ブロック図である。図 11 に示した実施の形態 2 の配信サーバ 11 の構成と異なる点は、データ処理部 310 は、公開復号鍵  $KP_{master}$  を保持する  $KP_{master}$  保持部 324 と、 $KP_{master}$  保持部 324 から出力される公開復号鍵  $KP_{master}$  に基づいて、通信網から通信装置 350 を介してデータバス  $BS1$  に与えられるデータを復号するための復号処理部 326 とをさらに備える構成となっている点である。暗号化処理部 316 は、復号処理部 326 での復号処理により抽出された公開暗号化鍵  $KP_{media}$  により、 $Ks$  発生部 314 で発生されたセッションキー  $Ks$  を暗号化し、また、配信制御部 312 は、復号処理部 326 での復号処理により抽出された証明データ  $Crtf$  により、配信を求めてきたメモリカードおよび携帯電話機が正規であるかの認証を行なう。

【0292】

配信サーバ 12 のその他の点は、図 12 に示した実施の形態 2 の配信サーバ 11 の構成の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

【0293】

図 34 は、本発明の実施の形態 5 のメモリカード 140 の構成を説明するための概略ブロック図であり、実施の形態 2 の図 13 と対比される図である。

【0294】

実施の形態 5 のメモリカード 140 の構成が、実施の形態 2 のメモリカード 120 の構成と異なる点は、まず、メモリカード 140 は、公開暗号鍵  $KP_{media}$  および証明データ  $Crtf$  とを公開復号鍵（公開認証鍵） $KP_{master}$  により暗号化された形で記録保持する  $[KP_{media}, Crtf]$   $KP_{master}$  保持部 1442 を備える構成となっていることである。一方で、切換えス

イッチ1436は省略され、[K P m e d i a, C r t f] K P m a s t e r 保持部1442の出力は直接データバスB S 3に与えられる。

【0295】

さらに、メモ리카ード140は、公開復号鍵K P m a s t e r を記録保持するためのK P m a s t e r 保持部1450と、K P m a s t e r 保持部1450から出力される公開復号鍵K P m a s t e r に基づいて、データバスB S 3上のデータを復号するための復号処理部1452とを備える。

【0296】

復号処理部1452での復号処理により抽出される公開暗号化鍵K P m e d i a および証明データC r t f のうち、公開暗号化鍵K P m e d i a は、暗号化処理部1430に与えられ、証明データC r t f は、データバスB S 5を介して、コントローラ1420に与えられる。

【0297】

メモ리카ード140のその他の構成は、図13に示したメモ리카ード120の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

【0298】

【配信モード】

図35および図36は、図34で説明したメモ리카ード140を用いた配信モードを説明するための第1および第2のフローチャートである。

【0299】

図35および図36においても、ユーザ1が、メモ리카ード140を装着した携帯電話機105にて配信サーバ12からコンテンツデータの配信を受ける場合の動作を説明している。

【0300】

まず、ユーザ1の携帯電話機105から、ユーザによりタッチキー1108のキーボタンの操作等によって、配信リクエストがなされる（ステップS100）。

【0301】

また、メモリカード140において保持される公開暗号化鍵KPmediaは、他のメモリカードにおける公開暗号化鍵KPmediaと区別するために公開暗号化鍵KPmedia(1)としている。さらに、メモリカード140、携帯電話機105における証明データをそれぞれCrtf(1)、Crtf(p)とする。

#### 【0302】

メモリカード140においては、この配信リクエストに応じて、[KPmedia, Crtf] KPmaster保持部1442から、公開暗号化鍵KPmedia(1)および証明データCrtf(1)を暗号化したデータ[KPmedia(1), Crtf(1)] KPmasterを携帯電話機105に対して出力する(ステップS102')。

#### 【0303】

携帯電話機105では、メモリカード140からのデータ[KPmedia(1), Crtf(1)] KPmasterとともに、[KPP, Crtf] KPmaster保持部1525からのデータ[KPP, Crtf(p)] KPmaster、配信リクエストを配信サーバ12に対して送信する(ステップS103)。

#### 【0304】

配信サーバ12では、メモリカード140から転送された配信リクエストならびにデータ[KPP, Crtf(p)] KPmaster、[KPmedia(1), Crtf(1)] KPmasterを受信すると(ステップS104')、公開復号鍵KPmasterにより復号処理部326が復号処理を行い、証明データCrtf(1)、Crtf(p)、公開暗号化鍵KPP、公開暗号化鍵KPmedia(1)の抽出を行なう(ステップS105)。

#### 【0305】

復号された証明データCrtf(1)およびCrtf(p)に基づいて、配信制御部312は、配信サーバ12に対して照会を行ない、メモリカードと携帯電話機の証明データCrtf(1)およびCrtf(p)がともに正規の証明データの場合は次の処理に移行し(ステップS106')、いずれかが正規の証明デ

ータでない場合には、処理を終了する（ステップS154）。

【0306】

照会の結果、正規の証明データであることが確認されると、配信サーバ12では、セッションキー発生部314が、セッションキーKsを生成する。さらに、配信サーバ12内の暗号化処理部316が、受信した公開暗号化鍵K<sub>Pmedia</sub>(1)により、このセッションキーKsを暗号化して暗号化セッションキー[Ks]K<sub>media</sub>(1)を生成する（ステップS108）。

【0307】

続いて、配信サーバ12は、暗号化セッションキー[Ks]K<sub>media</sub>(1)をデータバスBS1に与える。通信装置350は、暗号化処理部316からの暗号化セッションキー[Ks]K<sub>media</sub>(1)を、通信網を通じて、携帯電話機105のメモリカード140に対して送信する（ステップS110）。

【0308】

携帯電話機105が、暗号化セッションキー[Ks]K<sub>media</sub>(1)を受信すると（ステップS112）、メモリカード140においては、メモリインタフェース1200を介して、データバスBS3に与えられた受信データを、復号処理部1404が、秘密復号鍵K<sub>media</sub>(1)で復号処理することにより、セッションキーKsを復号し抽出する（ステップS114）。

【0309】

さらに、メモリカード140においては、Ks1発生部1432によりセッションキーKs1が生成される（ステップS115）。

【0310】

続いて、配信モードにおいては、切換スイッチ1409は、接点PaまたはPbが順次閉じる状態が選択されるので、暗号化処理部1406は、接点Paを介してセッションキー発生部1432から与えられるセッションキーKs1と接点Pbを介してKPcard(1)保持部1405から与えられる公開暗号化鍵K<sub>Pcard</sub>(1)（メモリカード140に対する公開暗号化鍵）とを、セッションキーKsにより暗号化し（ステップS116）、データ[KPcard(1)、Ks1]Ksを生成する（ステップS118）。

## 【0311】

携帯電話機105は、暗号化処理部1406により暗号化されたデータ[KPcard(1)、Ks1] Ksを配信サーバ12に対して送信する(ステップS120)。

## 【0312】

配信サーバ12では、通信装置350によりデータ[KPcard(1)、Ks1] Ksが受信され(ステップS122)、データバスBS1に与えられたデータ[KPcard(1)、Ks1] Ksを復号処理部318が、セッションキーKsにより復号処理して、公開暗号化鍵KPcard(1)およびセッションキーKs1を復号抽出する(ステップS124)。

## 【0313】

続いて、配信制御部312は、配信情報データベース304等に保持されているデータを元に、ライセンスIDデータ等を含むライセンス情報データLicenseを生成する(ステップS126)。

## 【0314】

さらに、配信サーバ12は、暗号化コンテンツデータ[Dc] Kcを配信情報データベース304より取得して、通信装置350を介して、メモリカード140に送信する(ステップS128)。

## 【0315】

携帯電話機105が暗号化コンテンツデータ[Dc] Kcを受信すると(ステップS130)、メモリカード140においては、受信した暗号化コンテンツデータ[Dc] Kcをそのままメモリ1412に格納する(ステップS132)。

## 【0316】

一方、配信サーバ12は、ライセンスキーKcを配信情報データベース304より取得し(ステップS134)、暗号化処理部320は、配信制御部312からのライセンスキーKcとライセンス情報データLicenseとを、復号処理部318より与えられた公開暗号化鍵KPcard(1)により暗号化処理する(ステップS136)。

## 【0317】

暗号化処理部322は、暗号化処理部320により暗号化されたデータ[Kc, License]Kcard(1)を受取って、さらに、メモ리카ード140からのセッションキーKs1により暗号化したデータをデータバスBS1に与える。通信装置350は、暗号化処理部322により暗号化されたデータ[[Kc, License]Kcard(1)]Ks1をメモ리카ード140に対して送信する。

## 【0318】

携帯電話機105がデータ[[Kc, License]Kcard(1)]Ks1を受信すると(ステップS142)、メモ리카ード140においては、復号処理部1410が接点Pfを介してKs1発生部1432から与えられるセッションキーKs1により復号処理を行ない、データ[Kc, License]Kcard(1)を抽出し、メモリ1412に格納する(ステップS146)。

## 【0319】

さらに、メモ리카ード140においては、コントローラ1420により制御されて、復号処理部1416が、メモリ1412に格納されたデータ[Kc, License]Kcard(1)を復号し、復号されたライセンス情報データLicenseを、レジスタ1500に格納する(ステップ148)。

## 【0320】

以上のような動作により、メモ리카ード140自身が、暗号化コンテンツデータを送る側(配信サーバ12)に、公開暗号化鍵KPmedia(1)およびセッションキーKs1を送信した上で、配信を受けることができ、メモ리카ード140は、音楽を再生可能な状態となる。

## 【0321】

さらに、メモ리카ード140から配信サーバ12へは、配信受理が通知され、配信サーバ12で配信受理を受信すると(ステップS150)、課金データベース302にユーザ1の課金データが格納され(ステップS152)、処理が終了する(ステップS154)。

## 【0322】

以上のような配信モードでは、メモ리카ードおよび携帯電話機の認証がなされ



た上でコンテンツデータの配信が行われるので、システムのセキュリティおよび著作権の保護がより強化される。

【0323】

〔再生モード〕

図37および図38は、携帯電話機105内において、メモリカード140に保持された暗号化コンテンツデータから、音楽信号を復号化し、音楽として外部に出力するための再生処理を説明する第1および第2のフローチャートである。

【0324】

図37および図38を参照して、携帯電話機105のタッチキー1108等からのユーザ1の指示により、再生リクエストが携帯電話機105に対して出力される（ステップS200）。

【0325】

これに応じて携帯電話機105からは、メモリカード140に対して、データ[KPp, Crtf(p)] KPmasterが送信される（ステップS241）。

【0326】

メモリカード140においては、データ[KPp, Crtf(p)] KPmasterを受信すると、復号処理部1452により復号処理が行われ、公開暗号化鍵KPpおよびデータCrtfの抽出が行われる（ステップS243）。

【0327】

抽出された証明データCrtfに基づいて、コントローラ1420は、携帯電話機105が正規の機器であるかを判断し（ステップS245）、正規の機器と判断した場合は、処理は次のステップS246に移行し、正規の機器でないと判断した場合は、処理を終了する（ステップS280）。

【0328】

正規の機器であると判断された場合、メモリカード140では、セッションキーKs1を生成する（ステップS246）。メモリカード140は、さらに、抽出された公開暗号化鍵KPpによりセッションキーKs1を暗号化し（ステップS248）、生成された暗号化セッションキー[Ks1] Kpを携帯電話機10

5に対して送信する（ステップS250）。

【0329】

携帯電話機105では、メモリカード140からの暗号化セッションキー [K<sub>s</sub>1] K<sub>p</sub>を受信すると、復号処理部1522が、秘密復号鍵K<sub>p</sub>により復号化してメモリカード140で生成したセッションキーK<sub>s</sub>1を抽出する（ステップS252）。続いて、K<sub>s</sub>発生部1502がセッションキーK<sub>s</sub>を生成し（ステップS253）、携帯電話機105の暗号化処理部1504は、携帯電話機105で生成したセッションキーK<sub>s</sub>をセッションキーK<sub>s</sub>1により暗号化して、暗号化セッションキー [K<sub>s</sub>] K<sub>s</sub>1を生成し（ステップS254）、この暗号化セッションキー [K<sub>s</sub>] K<sub>s</sub>1をメモリカード140に対して送信する（ステップS256）。

【0330】

メモリカード140は、データバスBS2を介して、携帯電話機105により生成され、かつ暗号化されたセッションキーK<sub>s</sub>を受け取り、セッションキーK<sub>s</sub>1により復号し、携帯電話機105で生成したセッションキーK<sub>s</sub>を抽出する（ステップS258）。

【0331】

続いて、メモリカード140において、コントローラ1420は、レジスタ1500に保持されるライセンス情報データLicenseに基づいて、復号可能であるかを判断し（ステップS259）、復号可能と判断した場合は、次の処理に移行し、復号不可能と判断した場合は、処理を終了する（ステップS280）。

【0332】

続いて、メモリカード140は、メモリ1412から、暗号化されているデータ [K<sub>c</sub>, License] Kcard (1)を読み出し、復号処理部1416が復号処理を行なう（ステップS260）。

【0333】

秘密復号鍵Kcard (1)により、メモリ1412から読み出されたデータを復号可能な場合（ステップS262）、ライセンスキーK<sub>c</sub>が抽出される（ス

テップS264)。一方、復号不可能の場合、処理は終了する（ステップS280）。

【0334】

メモリ1412から読み出されたデータを復号可能な場合は、さらに、レジスタ1500内のライセンス情報データLicenseのうち、再生回数に関するデータが変更される（ステップS266）。

【0335】

続いて、メモリカード140においては、暗号化処理部1406が、抽出したセッションキーKsにより、ライセンスキーKcを暗号化し（ステップS268）、暗号化されたライセンスキー[Kc]KsをデータバスBS2に与える（ステップS270）。

【0336】

携帯電話機105の復号処理部1506は、セッションキーKsにより復号化処理を行なうことにより、ライセンスキーKcを取得する（ステップS272）。

【0337】

続いて、メモリカード140は、暗号化コンテンツデータ[Dc]Kcをメモリ1412から読み出し、データバスBS2に与える（ステップS274）。

【0338】

携帯電話機105の音楽再生部1508は、暗号化コンテンツデータ[Dc]Kcを、抽出されたライセンスキーKcにより復号処理して平文のコンテンツデータを生成し（ステップS276）、コンテンツデータから音楽信号を再生して混合部1510に与える（ステップS276）。デジタルアナログ変換部1512は、混合部1510からのデータを受け取って変換し、外部に再生された音楽を出力し、処理が終了する（ステップS232）。

【0339】

このような構成とすることで、メモリカード自身および携帯電話自身が、それぞれセッションキーKs1またはKsを生成し、これにより暗号化コンテンツデータの授受を行なった上で、再生動作を行なうことが可能となる。

## 【0340】

さらに、メモリカード140が携帯電話機105の認証を行なった上で、再生動作を行なうため、システムのセキュリティおよび著作権の保護が向上する。

## 【0341】

## 〔移動または複製モード〕

図39および図40は、2つのメモリカード間において、コンテンツデータおよびキーデータ等の移動または複製を行なう処理を説明するための第1および第2のフローチャートである。

## 【0342】

まず、携帯電話機105と同様の構成を有する携帯電話機106が送信側であり、携帯電話機105が受信側であるものとする。また、携帯電話機106にも、メモリカード140と同様の構成を有するメモリカード142が装着されているものとする。

## 【0343】

携帯電話機106は、まず、携帯電話機105に対して、移動リクエストまたは複製リクエストを出力する（ステップS300）。

## 【0344】

携帯電話機105がこのリクエストを受信すると（ステップS301）、メモリカード142は、これに応じて、メモリ1412内の暗号化コンテンツデータ[Dc]Kcを読み出して、メモリカード140に対して出力し（ステップS302）、メモリカード140では、暗号化コンテンツデータ[Dc]Kcをメモリ1412に格納する（ステップS304）。

## 【0345】

続いて、携帯電話機106および105においては、ステップS300において与えられたリクエストが、「移動リクエスト」であるか「複製リクエスト」であるかが判断され（ステップS306、ステップS306'）、「移動リクエスト」である場合、メモリカード140は、この移動リクエストに応じて、[KPmedia, Crtf] KPmaster保持部1442から、公開暗号化鍵KPmedia(1)および証明データCrtf(1)を暗号化したデータ[KP

media (1), Crtf (1)] KPmaster を携帯電話機 105 に対して出力する (ステップ S307)。

【0346】

携帯電話機 105 では、メモ리카ード 140 からのデータ [KPmedia (1), Crtf (1)] KPmaster を携帯電話機 106 に対して送信する (ステップ S308)。

【0347】

携帯電話機 106 では、メモ리카ード 140 から転送されたデータ [KPmedia (1), Crtf (1)] KPmaster を受信すると (ステップ S309)、メモ리카ード 142 内の復号処理部 1452 が復号処理を行い、証明データ Crtf (1)、公開暗号化鍵 KPmedia (1) の抽出を行なう (ステップ S310)。

【0348】

復号された証明データ Crtf (1) に基づいて、コントローラ 1420 は、認証を行ない、正規メモ리카ードからのアクセスの場合は次の処理に移行し (ステップ S311)、正規メモ리카ードでない場合には、携帯電話機 106 は移動不可の通知を送信するとともに、メモ리카ード 142 は処理を終了する (ステップ S374)。携帯電話機 105 が移動不可通知を受信すると (ステップ S313)、メモ리카ード 140 も処理を終了する (ステップ S374)。

【0349】

一方、ステップ S311 での照会の結果、正規メモ리카ードであることが確認されると、メモ리카ード 142 の Ks2 発生回路 1432 は、セッションキー Ks2 を生成し (ステップ S314)、公開暗号化鍵 KPmedia (1) を用いて、暗号化処理部 1430 がセッションキー Ks2 を暗号化する (ステップ S315)。

【0350】

携帯電話機 106 は、暗号化セッションキー [Ks2] KPmedia (1) を携帯電話機 105 に対して送信する (ステップ S316)。携帯電話機 105 は、暗号化セッションキー [Ks2] KPmedia (1) を受信すると (ステ

ップS318)、メモリカード140に伝達し、メモリカード140は、復号処理部1404が復号して、セッションキーKs2を受理する(ステップS320)。さらに、メモリカード140においてセッションキーKs1が生成される(ステップS321)。

【0351】

メモリカード140においては、セッションキーKs2によりメモリカード140の公開暗号化鍵KPcard(1)およびセッションキーKs1を暗号化して(ステップS322)、携帯電話機105から携帯電話機106に対して暗号化されたデータ[KPcard(1)、Ks1]Ks2を送信する(ステップS324)。携帯電話機106は、データ[KPcard(1)、Ks1]Ks2を受信し(ステップS326)、メモリカード142に転送する。

【0352】

メモリカード142においては、復号処理部1410が、メモリカード140から送信された暗号化データ[KPcard(1)、Ks1]Ks2をセッションキーKs2により復号化して、メモリカード140の公開暗号化鍵KPcard(1)、セッションキーKs1を復号抽出する(ステップS330)。

【0353】

続いて、メモリカード142においては、メモリ1412からメモリカード142の公開暗号化鍵KPcard(2)により暗号化されているライセンスキーKc、ライセンス情報データLicenseに対応する[Kc、License]Kcard(2)読出される(ステップS332)。

【0354】

続いて、メモリカード142の復号処理部1416が、秘密復号鍵Kcard(2)により、ライセンスキーKc、ライセンス情報データLicenseを復号処理する(ステップS334)。

【0355】

メモリカード142のコントローラ1420は、このようにして復号されたライセンス情報データLicenseの値を、レジスタ1500内のデータ値と置換する(ステップS336)。

## 【0356】

さらに、メモリカード142の暗号化処理部1414は、復号処理部1410において抽出されたメモリカード140における公開暗号化鍵K P c a r d (1)により、ライセンスキーK c、ライセンス情報データL i c e n s eとを暗号化する(ステップS338)。

## 【0357】

メモリカード142の暗号化処理部1414により暗号化されたデータは、切換スイッチ1409(接点P dが閉じている)を介して、さらに、暗号化処理部1406に与えられ、メモリカード142の暗号化処理部1406は、データ[K c, L i c e n s e] K c a r d (1)をセッションキーK s 1により暗号化してデータ[[K c, L i c e n s e] K c a r d (1)] K s 1を生成する(ステップS340)。

## 【0358】

続いて、メモリカード142は、携帯電話機106に対してデータ[[K c, L i c e n s e] K c a r d (1)] K s 1を出力し(ステップS342)、携帯電話機106はデータ[[K c, L i c e n s e] K c a r d (1)] K s 1を携帯電話機105に対して送信する(ステップS344)。

## 【0359】

携帯電話機105が受信したデータ[[K c, L i c e n s e] K c a r d (1)] K s 1は(ステップS346)、メモリカード140に対して伝達され、メモリカード140の復号処理部1410は、暗号化されたデータ[[K c, L i c e n s e] K c a r d (1)] K s 1を復号して、データ[K c, L i c e n s e] K c a r d (1)を受理する(ステップS348)。

## 【0360】

メモリカード140においては、復号処理部1410により、セッションキーK s 1に基づいて復号化処理されたデータ[K c, L i c e n s e] K c a r d (1)をメモリ1412に格納する(ステップS350)。さらに、メモリカード140においては、復号処理部1416が、秘密復号鍵K c a r d (1)に基づいて、データ[K c, L i c e n s e] K c a r d (1)を復号し、復号され

たライセンス情報データLicenseをレジスタ1500に格納する（ステップS352）。

【0361】

以後の移動モードにおける処理ならびに複製モードにおけるメモ리카ード140および142の処理は、図18および図19で説明した実施の形態2のメモ리카ード120、122等の処理と同様であるので、その説明は繰り返さない。

【0362】

このような構成とすることで、移動元および移動先のメモ리카ード自身が、セッションキーをそれぞれ生成した上で、移動動作を行なうこと、および複製動作を行なうことが可能となる。

【0363】

したがって、データバス上で伝達されるデータの暗号化キーが、セッションごとに、かつ、機器ごとに変更されるので、データ授受のセキュリティが一層向上するという効果がある。

【0364】

しかも、以上のような構成を用いることで、たとえば、メモ리카ード142からメモ리카ード140へのデータの移動を、上述したようなセッションキー発生回路1502を有する携帯電話端末を介さずに、メモ리카ードとメモ리카ードとを接続可能なインターフェース機器により行なうことも可能となり、ユーザの利便性が一層向上するという効果がある。

【0365】

ここで、移動モード時には、再生情報内の再生回数を制限するライセンス情報データについては、メモリ1412に記録されたライセンス情報データを、レジスタ1500にて再生の都度修正された再生回数を記録したライセンス情報データに変更することでライセンス情報データを更新する。このようにして、メモ리카ード間をコンテンツデータが移動しても、再生回数に制限があるコンテンツデータの再生回数は、配信時に決められた再生回数の制限を越えることがないようにすることが可能である。

【0366】



しかも、メモリカード142がメモリカード140の認証を行った上で、移動動作を行なうため、システムのセキュリティおよび著作権の保護が向上する。

【0367】

〔実施の形態6〕

図41は、本発明の実施の形態6のコンテンツデータ販売機3010の構成を示す概略ブロック図であり、実施の形態4の図27と対比される図である。

【0368】

ただし、以下の説明では、実施の形態5で説明したメモリカード140との間のインターフェースのためにメモリスロット2030を設ける構成とし、実施の形態4の変形例と同様に、携帯電話機105を介することなく、メモリカード140とコンテンツデータ販売機3010とが直接データの授受を行なう構成であるものとする。

【0369】

もちろん、コネクタ2010により、携帯電話機105を介して、メモリカード140とコンテンツデータ販売機3010とがデータの授受を行なう構成とすることも可能である。

【0370】

したがって、コンテンツデータ販売機3010の構成が、実施の形態4のコンテンツデータ販売機3000の構成と異なる点は、コネクタ2010の代わりに、メモリスロット2030が設けられていることと、データ処理部2100は、公開復号鍵K P m a s t e r を保持するK P m a s t e r 保持部324と、K P m a s t e r 保持部324から出力される公開復号鍵K P m a s t e r に基づいて、通信網から通信装置350を介してデータバスB S 1に与えられるデータを復号するための復号処理部326とをさらに備える構成となっている点である。暗号化処理部316は、復号処理部326での復号処理により抽出された公開暗号化鍵K P m e d i a により、K s 発生部314で発生されたセッションキーK s を暗号化し、また、配信制御部312は、復号処理部326での復号処理により抽出された証明データC r t f により、配信を求めてきたメモリカードが正規のメモリカードであるかの認証を行なう。

【0371】

コンテンツデータ販売機3010のその他の点は、図27に示した実施の形態4のコンテンツデータ販売機3000の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

【0372】

〔配信モード〕

図42および図43は、図41で説明したコンテンツデータ販売機3010を用いたデータ配信システムにおける配信動作を説明するための第1および第2のフローチャートである。

【0373】

図42および図43においては、ユーザ1が、メモ리카ード140を用いることで、コンテンツデータ販売機3010からコンテンツデータ（音楽データ）の配信を受ける場合の動作を説明している。

【0374】

まず、ユーザが、コンテンツデータ販売機3010のキーボード2004のキーボタンの操作等によって、配信リクエストを指示する（ステップS500）。

【0375】

コンテンツデータ販売機3010からは、メモ리카ード140に対して、認証のためのデータ〔K P m e d i a , C r t f〕K P m a s t e rの送信依頼が出力される（ステップS502'）。

【0376】

メモ리카ード140においては、この送信依頼に応じて、〔K P m e d i a , C r t f〕K P m a s t e r保持部1442から、公開暗号化鍵K P m e d i a (1) および証明データC r t f (1)を暗号化したデータ〔K P m e d i a (1), C r t f (1)〕K P m a s t e rをコンテンツデータ販売機3010に対して出力する（ステップS507）。

【0377】

コンテンツデータ販売機3010では、メモ리카ード140から転送されたデータ〔K P m e d i a (1), C r t f (1)〕K P m a s t e rを受信すると

、公開復号鍵K P m a s t e rにより復号処理部326が復号処理を行い、証明データC r t f (1)、公開暗号化鍵K P p、公開暗号化鍵K P m e d i a (1)の抽出を行なう(ステップS509)。

【0378】

復号された証明データC r t f (1)に基づいて、配信制御部312は、正規メモリカードからのアクセスかどうかの判断を行なう。正規のメモリカードの場合は次の処理に移行し(ステップS511)、正規メモリカードでない場合には、管理サーバ2200中の管理データベースに異常終了記録を格納し(ステップS561)、処理を終了する(ステップS562)。

【0379】

コンテンツデータ販売機3010は、ステップS511での照会の結果、正規メモリカードであることが確認されると、ディスプレイ2002を介してユーザーに料金投入を案内し、料金徴収を行なう(ステップS512)。

【0380】

続いて、コンテンツデータ販売機3010は、セッションキー発生部314が、セッションキーK sを生成する。さらに、コンテンツデータ販売機3010内の暗号化処理部316が、受信した公開暗号化鍵K P m e d i a (1)により、このセッションキーK sを暗号化して暗号化セッションキー[K s] K m e d i a (1)を生成する(ステップS514)。

【0381】

続いて、コンテンツデータ販売機3010は、暗号化セッションキー[K s] K m e d i a (1)をデータバスB S 1に与え、カードスロット2030から出力する(ステップS516)。

【0382】

メモリカード140においては、メモリインタフェース1200を介して、データバスB S 3に与えられた暗号化セッションキー[K s] K m e d i a (1)を、復号処理部1404が、秘密復号鍵K m e d i a (1)により復号処理することにより、セッションキーK sを復号し抽出する(ステップS520)。さらに、メモリカード140では、セッションキーK s 1が生成される(ステップS

521)。

【0383】

続いて、配信モードにおいては、切換スイッチ1408は、接点Paが閉じる状態が選択されているので、暗号化処理部1406は、接点Paを介してKPcard(1)保持部1405から与えられる公開暗号化鍵KPcard(1)を、セッションキーKsにより暗号化し(ステップS522)、データ[KPcard(1)]Ksを生成する(ステップS524)。

【0384】

コンテンツデータ販売機3010では、カードスロット2030を介してデータ[KPcard(1)]Ksが受信され(ステップS528)、データバスBS1に与えられたデータ[KPcard(1)]Ksを復号処理部318が、セッションキーKsにより復号処理して、公開暗号化鍵KPcard(1)を復号抽出する(ステップS530)。

【0385】

続いて、配信制御部312は、配信情報データベース304等に保持されているデータを元に、ライセンスIDデータ等を含むライセンス情報データLicenseを生成する(ステップS532)。

【0386】

さらに、コンテンツデータ販売機3010は、暗号化コンテンツデータ[Dc]Kcを配信情報データベース304より取得して、カードスロット2030を介して、メモリカード140に送信する(ステップS534)。

【0387】

メモリカード140においては、受信した暗号化コンテンツデータ[Dc]Kcをそのままメモリ1412に格納する(ステップS538)。

【0388】

一方、コンテンツデータ販売機3010は、ライセンスキーKcを配信情報データベース304より取得し(ステップS540)、暗号化処理部320は、配信制御部312からのライセンスキーKcとライセンス情報データLicenseとを、復号処理部318より与えられた公開暗号化鍵KPcard(1)によ

り暗号化処理する（ステップ S 5 4 2）。

【0 3 8 9】

暗号化処理部 3 2 2 は、暗号化処理部 3 2 0 により暗号化されたデータ [K c、L i c e n s e] K c a r d (1) を受取って、さらにセッションキー K s により暗号化したデータをデータバス B S 1 に与え、暗号化処理部 3 2 2 により暗号化されたデータ [ [K c、L i c e n s e] K c a r d (1) ] K s 1 がメモ리카ード 1 4 0 に対して送信される（ステップ S 5 4 6）。

【0 3 9 0】

メモ리카ード 1 4 0 においては、復号処理部 1 4 1 0 がセッションキー K s 1 により復号処理を行ない、データ [K c、L i c e n s e] K c a r d (1) を抽出し、メモリ 1 4 1 2 に格納する（ステップ S 5 5 2）。

【0 3 9 1】

さらに、メモ리카ード 1 4 0 においては、コントローラ 1 4 2 0 により制御されて、復号処理部 1 4 1 6 が、メモリ 1 4 1 2 に格納されたデータ [K c、L i c e n s e] K c a r d (1) を復号し、復号されたライセンス情報データ L i c e n s e を、レジスタ 1 5 0 0 に格納する（ステップ S 5 5 4）。

【0 3 9 2】

以上のような動作により、メモ리카ード 1 4 0 は、コンテンツデータから音楽を再生可能な状態となる。

【0 3 9 3】

さらに、メモ리카ード 1 4 0 からコンテンツデータ販売機 3 0 1 0 へは、配信受理が通知され（ステップ S 5 5 8）、コンテンツデータ販売機 3 0 1 0 で配信受理を受信すると、管理サーバ 2 2 0 0 中の管理データベースに販売記録が送信され（ステップ S 5 6 0）、処理が終了する（ステップ S 5 6 2）。

【0 3 9 4】

以上のような構成により、ユーザは、より簡易に暗号化された音楽データ等のコンテンツデータの配信を受けることができる。しかも、メモ리카ードの認証がなされた上でコンテンツデータの配信が行われるので、システムのセキュリティおよび著作権の保護がより強化される。

【0395】

〔実施の形態7〕

図44は、実施の形態7における携帯電話機107の構成を説明するための概略ブロック図である。

【0396】

図32に示した実施の形態5の携帯電話機105の構成と異なる点は、携帯電話機という再生装置に共通な復号鍵Kcomを保持するKcom保持部1530と、復号処理部1506の出力を受けて、復号鍵Kcomについて復号し、音楽再生部1508にライセンスキーKcを与える復号処理部1532とを備える構成となっていることである。

【0397】

携帯電話機107のその他の点は、図32に示した実施の形態5の携帯電話機105の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。メモリカード140の構成も同様である。

【0398】

すなわち、実施の形態7では、実施の形態5において、音楽再生部1508に最終的にライセンスキーKcと与えられる以前において、システムを構成する機器間で授受されていたライセンスキーKcを、実施の形態7では、さらに暗号化した〔Kc〕Kcomという状態でやり取りする以外は、実施の形態5の構成と同様である。

【0399】

なお、以下の説明では、復号鍵Kcomは共通鍵であるものとして説明するが、本発明はこのような場合に限定されず、たとえば、暗号化は公開鍵Kpcomで行い、復号化を公開暗号化鍵Kpcomとは非対称な秘密復号鍵Kcomで行なう構成としてもよい。

【0400】

図45は、実施の形態7の携帯電話機107に対応した配信サーバ13の構成を示す概略ブロック図である。図33に示した実施の形態5の配信サーバ12の構成と異なる点は、データ処理部310は、復号鍵Kcomを保持するKcom

保持部 330 と、配信制御部 312 を介して配信情報データベース 304 から与えられるライセンスキー Kc を復号鍵 Kcom により暗号化処理して、暗号化ライセンスキー [Kc] Kcom として暗号化処理部 320 に与える暗号化処理部 332 をさらに備える構成となっている点である。

#### 【0401】

配信サーバ 13 のその他の点は、図 33 に示した実施の形態 5 の配信サーバ 12 の構成の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

#### 【0402】

##### 【配信モード】

図 46 および図 47 は、図 44 および 45 で説明した配信サーバ 13 と携帯電話機 107 を用いた配信モードを説明するための第 1 および第 2 のフローチャートである。

#### 【0403】

図 46 および図 47 においても、ユーザ 1 が、メモリカード 140 を用いることで、配信サーバ 13 からコンテンツデータ（音楽データ）の配信を受ける場合の動作を説明している。

#### 【0404】

ただし、図 46 および図 47 の処理は、ステップ S134 において、配信サーバ 13 が、ライセンスキー Kc を配信情報データベース 304 より取得した後、暗号化処理部 332 がキー Kc を暗号化して（ステップ S135）、以後は、暗号化ライセンスキー [Kc] Kcom として授受される点を除いては、図 35 および図 36 で説明した実施の形態 5 の配信モードと同様であるので、その説明は繰り返さない。

#### 【0405】

以上のような配信モードでは、実施の形態 5 に比べて、さらにシステムのセキュリティが強化される。

#### 【0406】

##### 【再生動作】

図48および図49は、携帯電話機107内において、メモリカード140に保持された暗号化コンテンツデータから、音楽信号を再生し、音楽として外部に出力するための再生処理を説明する第1および第2のフローチャートである。

【0407】

ただし、図48および図49に示した再生処理は、ステップS264でメモリカード140のメモリ1412から読み出されるキーが、暗号化ライセンスキー [Kc] Kcomであり、以後、暗号化ライセンスキー [Kc] Kcomとして携帯電話機107に送信され、携帯電話機107において、ステップS273で復号処理部1532によりキー [Kc] Kcomが復号されライセンスキーKcが音楽再生部1508に与えられる点以外は、図37および図38に示した実施の形態5の再生処理と同様であるのでその説明は繰り返さない。

【0408】

このような構成とすることで、再生モードにおけるシステムのセキュリティおよび著作権の保護が一層向上する。

【0409】

〔移動または複製モード〕

図50および図51は、実施の形態7において、2つのメモリカード間において、コンテンツデータおよびキーデータ等の移動または複製を行なう処理を説明するための第1および第2のフローチャートである。

【0410】

ただし、図50および図51の処理は、ライセンスキーKcが、暗号化ライセンスキー [Kc] Kcomとして授受される点を除いては、図39および図40で説明した実施の形態5の移動または複製モードの動作と同様であるので、その説明は繰り返さない。

【0411】

このような構成とすることで、移動または複製モードにおけるシステムのセキュリティおよび著作権の保護が一層向上する。

【0412】

〔実施の形態8〕



図 5 2 は、本発明の実施の形態 8 のコンテンツデータ販売機 3 0 2 0 の構成を示す概略ブロック図であり、実施の形態 6 の図 4 1 と対比される図である。

【0 4 1 3】

コンテンツデータ販売機 3 0 2 0 の構成が、実施の形態 6 のコンテンツデータ販売機 3 0 1 0 の構成と異なる点は、データ処理部 2 1 0 0 は、復号鍵 K c o m を保持する K c o m 保持部 3 3 0 と、配信制御部 3 1 2 を介して配信情報データベース 3 0 4 から与えられるライセンスキー K c を復号鍵 K c o m により暗号化処理して、暗号化ライセンスキー [K c] K c o m として暗号化処理部 3 2 0 に与える暗号化処理部 3 3 2 をさらに備える構成となっている点である。

【0 4 1 4】

コンテンツデータ販売機 3 0 2 0 のその他の点は、図 4 1 に示した実施の形態 6 のコンテンツデータ販売機 3 0 1 0 の構成の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

【0 4 1 5】

もちろん、実施の形態 8 でも、コネクタ 2 0 1 0 により、携帯電話機 1 0 7 を介して、メモリカード 1 4 0 とコンテンツデータ販売機 3 0 2 0 とがデータの授受を行なう構成とすることも可能である。

【0 4 1 6】

[配信モード]

図 5 3 および図 5 4 は、図 5 2 で説明したコンテンツデータ販売機 3 0 2 0 を用いたデータ配信システムにおける配信モードを説明するための第 1 および第 2 のフローチャートである。

【0 4 1 7】

図 5 3 および図 5 4 においては、ユーザ 1 が、メモリカード 1 4 0 を用いることで、コンテンツデータ販売機 3 0 2 0 からコンテンツデータ（音楽データ）の配信を受ける場合の動作を説明している。

【0 4 1 8】

ただし、図 5 3 および図 5 4 の処理は、ステップ S 5 4 0 において、コンテンツデータ販売機 3 0 2 0 が、ライセンスキー K c を配信情報データベース 3 0 4

より取得した後、暗号化処理部 332 がライセンスキー Kc を暗号化して（ステップ S541）、以後は、暗号化ライセンスキー [Kc] Kcom として授受される点を除いては、図 42 および図 43 で説明した実施の形態 5 の配信動作と同様であるので、その説明は繰り返さない。

#### 【0419】

以上のような配信モードでは、実施の形態 6 に比べて、さらにシステムのセキュリティが強化される。

#### 【0420】

ここでは暗号化コンテンツデータを配信し、メモリカード 110、120、140 内のメモリ 1412 に格納した後、ライセンスキー Kc、ライセンス情報データ License の配信を受けるように説明したが、逆にライセンスキー Kc、ライセンス情報データ License を配信し、メモリカード 110、120、140 内のレジスタ 1500 に格納した後、暗号化コンテンツデータの配信を受けても構わない。

#### 【0421】

さらに、移動モードにおいても配信モードと同様に、暗号化コンテンツデータ、ライセンスキー Kc、ライセンス情報データ License のいずれの移動が先であっても構わない。

#### 【0422】

なお、以上説明してきた各実施の形態において、配信データとしてコンテンツデータに付随する非暗号化データ、たとえば、上記音楽データの曲名、実演者（歌手、演奏家等）、作曲家、作詞家等の当該音楽データ（コンテンツデータ）に関する著作権情報や配信サーバ 10、11、コンテンツデータ販売機 3000、3001 に対してアクセスするための情報等を、付加データ Di として暗号化コンテンツデータと併せて配信することも可能である。この付加データ Di は、配信、移動、複製においてはコンテンツデータとともに処理され、再生時には分離されてコンテンツデータとは個別にアクセス可能となるように、暗号化コンテンツデータと同じメモリ 1412 に格納される。

#### 【0423】

## 【実施の形態 9】

図 55 は、以上説明してきたメモ리카ード 110, 120, 140 等の端子 1202 部分の構成を説明する概略ブロック図である。

## 【0424】

以下では、メモ리카ード 140 の端子 1202 部分の構成であるものとして説明する。

## 【0425】

メモ리카ード 140 には、端子 1202 からシリアルにデータやコマンドが与えられる。これに対して、メモ리카ード 140 中のデータバス BS3 には、パラレルにデータやコマンドが伝達されるものとする。

## 【0426】

図 55 は、このようなメモ리카ード 140 へのデータ入力時のシリアル・パラレル変換と、データ出力時のパラレル・シリアル変換を行なう構成を示す概略ブロック図である。

## 【0427】

端子 1202 中のデータピン 1460 には、データ入出力のタイミングを指定するための信号である信号 CS が与えられる。たとえば、信号 CS が活性化（“L” レベル）となった後の所定期間後に、データ入力ピン 1462 に与えられるデータが“L” レベルとなることで、データ入力のタイミングが検出される。どうように、信号 CS が活性化（“L” レベル）となった後の所定期間後に、データ出力ピン 1464 に出力されるデータが“L” レベルとなることで、データ出力のタイミングが検出される。インターフェースコントローラ 1490 は、メモ리카ード 140 の外部からデータバス BS3 へのデータ入力、およびデータバス BS3 からメモ리카ード 140 外部へのデータ出力を管理する。

## 【0428】

データ入力時は、データ入力ピン 1462 に与えられたデータは、バッファ 1468 を介して、縦列に接続された D-フリップフロップ 1470. 0~1470. 7 に入力される。すなわち、8ビット分のデータが入力された時点で、D-フリップフロップ 1470. 0~1470. 7 の全てのデータが更新され、その

時点で、インターフェースコントローラ1490により制御されて、データバッファ1427.0~1427.7からデータバスBS3へデータが平行に出力される。

#### 【0429】

データ出力時は、データバスBS3からのデータがマルチプレクサ1476.1~1476.7を介して、平行に与えられD-フリップフロップ1474.0~1474.7に格納される。その後インターフェースコントローラ1490により制御されて、マルチプレクサ1476.1~1476.7の接続が切り換えられ、D-フリップフロップ1474.0~1474.7が縦列に接続される。この状態で、D-フリップフロップ1474.0~1474.7のそれぞれに格納されたデータが、順次シリアルに、インターフェースコントローラ1490により制御される出力バッファ1470を介して、データ出力ピン1464から出力される。

#### 【0430】

##### 【実施の形態9の変形例】

図56は、データ入力速度を向上させるために、データ入力ピンの本数を1本から2本または4本に変更可変することが可能な、メモリカード140の端子1202部分の構成の変形例を説明するための概略ブロック図である。

#### 【0431】

図55に示した構成と異なる点は、まず、4本のデータ入力ピン1462.0~1462.3およびそれらに対応する入力バッファ1468.0~1468.3が設けられていることと、これらデータ入力ピン1462.0~1462.3に与えられたコマンドを入力バッファ1468.0~1468.3からインターフェースコントローラ1490に伝達するためのマルチプレクサ1467と、データ入力ピン1462.0~1462.3に与えられたデータまたはコマンドを、入力バッファ1468.0~1468.3からD-フリップフロップ1470.0~1470.7に選択的に与えるためのマルチプレクサ1469.1~1469.7とをさらに備える構成となっていることである。

#### 【0432】

次に動作について簡単に説明する。

電源投入後には、たとえば、メモ리카ード140は、1本のデータ入力ピン1462.0からのみデータ入力を受けつける状態となっている。

#### 【0433】

以下では、外部からデータ入力ピン1462.0～1462.3およびマルチプレクサ1467を経由してインターフェースコントローラ1490に与えられたコマンドにより、インターフェースコントローラ1490がマルチプレクサ1469.1～1469.7を制御することで、4本のデータ入力ピン1462.0～1462.3からのデータをパラレルに入力するモードに動作モードが変更されたものとする。

#### 【0434】

まず、第1のタイミングで4本のデータ入力ピン1462.0～1462.3に与えられたデータは、マルチプレクサ1469.1～1469.3を経由してD-フリップフロップ1470.0～1470.3に与えられる。

#### 【0435】

次の第2のタイミングで、マルチプレクサ1469.1～1469.7の接続が切替わり、D-フリップフロップ1470.0～1470.3の出力がそれぞれ、D-フリップフロップ1470.4～1470.7に与えられて格納される。さらに第3のタイミングで、4本のデータ入力ピン1462.0～1462.3に与えられたデータは、マルチプレクサ1469.1～1469.3を経由してD-フリップフロップ1470.0～1470.3に与えられる。

#### 【0436】

以上で、8ビット分のデータのD-フリップフロップ1470.0～1470.7への格納が終了する。以後は、図55の場合と同様に、データバスBS3に対してパラレルに8ビット分のデータが与えられる。

#### 【0437】

データ出力の際の動作は、図55の場合と同様である。

以上のような構成により、データ配信時、特にコンテンツデータ販売機2000等からコンテンツデータを購入する際のメモ리카ード140へのデータ配信時

間を短縮することが可能である。

【0438】

また、以上説明した各実施の形態のうち、2つの携帯電話にそれぞれ装着された2つのメモリカード間で、たとえば、PHSのトランシーバモード等を利用することにより、コンテンツデータの移動を行なう処理を説明した実施の形態においては、このような構成に限定されず、たとえば、1つの携帯電話機に複数のメモリカードが同時装着可能な場合は、当該携帯電話機に2つのメモリカードを同時に装着することで、コンテンツデータの移動を行なう構成とすることも可能である。このようなコンテンツデータの移動の場合は、以上説明した各実施の形態において、2つの携帯電話機間での送受信のやりとりを省略すればよい。

【0439】

今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は上記した説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

【0440】

【発明の効果】

以上説明したとおり、本願発明にかかる配信システムでは、正規のユーザのみがコンテンツデータを受信してメモリ中に格納することが可能となり、かつ、1度メモリカード中に格納されたデータを、他人にコピーさせる場合は、当該他人が再生可能な状態でデータを移植するためには、送信元においては、データの再生が不能になってしまう構成となっているので、無制限なコピーにより著作権が不当な不利益を被るのを防止することが可能となる。

【0441】

また、ユーザが配信キャリアを介してではなく、コンテンツデータ販売機により暗号化コンテンツデータを購入することができるので、ユーザの利便性が一層向上する。

【図面の簡単な説明】

【図1】 本発明の情報配信システムの全体構成を概略的に説明するための

概念図である。

【図 2】 図 1 に示した情報配信システムにおいて使用される通信のためのキーデータ（鍵データ）等の特性をまとめて説明する図である。

【図 3】 図 1 に示した配信サーバ 1 0 の構成を示す概略ブロック図である。

【図 4】 図 1 に示した携帯電話機 1 0 0 の構成を説明するための概略ブロック図である。

【図 5】 図 4 に示したメモリカード 1 1 0 の構成を説明するための概略ブロック図である。

【図 6】 図 1 および図 3 ～図 5 で説明したデータ配信システムにおける配信モードを説明するための第 1 のフローチャートである。

【図 7】 図 1 および図 3 ～図 5 で説明したデータ配信システムにおける配信モードを説明するための第 2 のフローチャートである。

【図 8】 携帯電話機 1 0 0 内においてコンテンツデータを再生し、音楽として外部に出力するための再生処理を説明するフローチャートである。

【図 9】 2 つのメモリカード間において、コンテンツデータおよびキーデータ等の移動または複製を行なう処理を説明するための第 1 のフローチャートである。

【図 1 0】 2 つのメモリカード間において、コンテンツデータおよびキーデータ等の移動または複製を行なう処理を説明するための第 2 のフローチャートである。

【図 1 1】 実施の形態 2 のメモリカード 1 2 0 に対応した音楽サーバ 3 1 の構成を示す概略ブロック図である。

【図 1 2】 実施の形態 2 における携帯電話機 1 0 1 の構成を説明するための概略ブロック図である。

【図 1 3】 本発明の実施の形態 2 のメモリカード 1 2 0 の構成を説明するための概略ブロック図である。

【図 1 4】 図 1 3 で説明したメモリカード 1 2 0 を用いた配信モードを説明するための第 1 のフローチャートである。

【図 1 5】 図 1 3 で説明したメモリカード 1 2 0 を用いた配信モードを説明するための第 2 のフローチャートである。

【図 1 6】 携帯電話機 1 0 1 内においてコンテンツデータを再生し、音楽として外部に出力するための再生処理を説明する第 1 のフローチャートである。

【図 1 7】 携帯電話機 1 0 1 内においてコンテンツデータを再生し、音楽として外部に出力するための再生処理を説明する第 2 のフローチャートである。

【図 1 8】 2 つのメモリカード間でコンテンツデータおよびキーデータ等の移動または複製を行なう処理を説明するための第 1 のフローチャートである。

【図 1 9】 2 つのメモリカード間でコンテンツデータおよびキーデータ等の移動または複製を行なう処理を説明するための第 2 のフローチャートである。

【図 2 0】 実施の形態 3 のデータ配信システムの構成を説明するための概念図である。

【図 2 1】 実施の形態 3 のコンテンツデータ販売機 2 0 0 0 の構成を示す概略ブロック図である。

【図 2 2】 図 2 0 および図 2 1 で説明したデータ配信システムにおける配信モードを説明するための第 1 のフローチャートである。

【図 2 3】 図 2 0 および図 2 1 で説明したデータ配信システムにおける配信モードを説明するための第 2 のフローチャートである。

【図 2 4】 実施の形態 3 の変形例のコンテンツデータ販売機 2 0 0 1 の構成を示す概念図である。

【図 2 5】 実施の形態 3 の変形例のデータ配信システムにおける配信モードを説明するための第 1 のフローチャートである。

【図 2 6】 実施の形態 3 の変形例のデータ配信システムにおける配信モードを説明するための第 2 のフローチャートである。

【図 2 7】 実施の形態 4 のコンテンツデータ販売機 3 0 0 0 の構成を説明するための概略ブロック図である。

【図 2 8】 図 2 7 で説明したデータ配信システムにおける配信モードを説明するための第 1 のフローチャートである。

【図 2 9】 図 2 7 で説明したデータ配信システムにおける配信モードを説



明するための第 2 のフローチャートである。

【図 3 0】 実施の形態 4 の変形例のデータ配信システムにおける配信モードを説明するための第 1 のフローチャートである。

【図 3 1】 実施の形態 4 の変形例のデータ配信システムにおける配信モードを説明するための第 2 のフローチャートである。

【図 3 2】 実施の形態 5 における携帯電話機 1 0 5 の構成を説明するための概略ブロック図である。

【図 3 3】 実施の形態 5 のメモリカード 1 4 0 に対応した配信サーバ 1 2 の構成を示す概略ブロック図である。

【図 3 4】 本発明の実施の形態 5 のメモリカード 1 4 0 の構成を説明するための概略ブロック図である。

【図 3 5】 メモリカード 1 4 0 を用いた配信モードを説明するための第 1 のフローチャートである。

【図 3 6】 メモリカード 1 4 0 を用いた配信モードを説明するための第 2 のフローチャートである。

【図 3 7】 メモリカード 1 4 0 に保持された暗号化コンテンツデータから、音楽として外部に出力するための再生処理を説明する第 1 のフローチャートである。

【図 3 8】 メモリカード 1 4 0 に保持された暗号化コンテンツデータから、音楽として外部に出力するための再生処理を説明する第 2 のフローチャートである。

【図 3 9】 2 つのメモリカード間において、コンテンツデータおよびキーデータ等の移動または複製を行なう処理を説明するための第 1 のフローチャートである。

【図 4 0】 2 つのメモリカード間において、コンテンツデータおよびキーデータ等の移動または複製を行なう処理を説明するための第 2 のフローチャートである。

【図 4 1】 本発明の実施の形態 6 のコンテンツデータ販売機 3 0 1 0 の構成を示す概略ブロック図である。

【図 4 2】 コンテンツデータ販売機 3 0 1 0 を用いたデータ配信システムにおける配信モードを説明するための第 1 のフローチャートである。

【図 4 3】 コンテンツデータ販売機 3 0 1 0 を用いたデータ配信システムにおける配信モードを説明するための第 2 のフローチャートである。

【図 4 4】 実施の形態 7 における携帯電話機 1 0 7 の構成を説明するための概略ブロック図である。

【図 4 5】 実施の形態 7 の携帯電話機 1 0 7 に対応した配信サーバ 1 3 の構成を示す概略ブロック図である。

【図 4 6】 配信サーバ 1 2 と携帯電話機 1 0 7 を用いた配信モードを説明するための第 1 のフローチャートである。

【図 4 7】 配信サーバ 1 2 と携帯電話機 1 0 7 を用いた配信モードを説明するための第 2 のフローチャートである。

【図 4 8】 メモリカード 1 4 0 に保持された暗号化コンテンツデータから、音楽として外部に出力するための再生処理を説明する第 1 のフローチャートである。

【図 4 9】 メモリカード 1 4 0 に保持された暗号化コンテンツデータから、音楽として外部に出力するための再生処理を説明する第 2 のフローチャートである。

【図 5 0】 実施の形態 7 において、2 つのメモリカード間において、コンテンツデータおよびキーデータ等の移動または複製を行なう処理を説明するための第 1 のフローチャートである。

【図 5 1】 実施の形態 7 において、2 つのメモリカード間において、コンテンツデータおよびキーデータ等の移動または複製を行なう処理を説明するための第 2 のフローチャートである。

【図 5 2】 本発明の実施の形態 8 のコンテンツデータ販売機 3 0 2 0 の構成を示す概略ブロック図である。

【図 5 3】 コンテンツデータ販売機 3 0 2 0 を用いたデータ配信システムにおける配信モードを説明するための第 1 のフローチャートである。

【図 5 4】 コンテンツデータ販売機 3 0 2 0 を用いたデータ配信システム

における配信モードを説明するための第2のフローチャートである。

【図55】 メモリカード140の端子1202部分の構成を説明する概略ブロック図である。

【図56】 メモリカード140の端子1202部分の構成の変形例を説明するための概略ブロック図である。

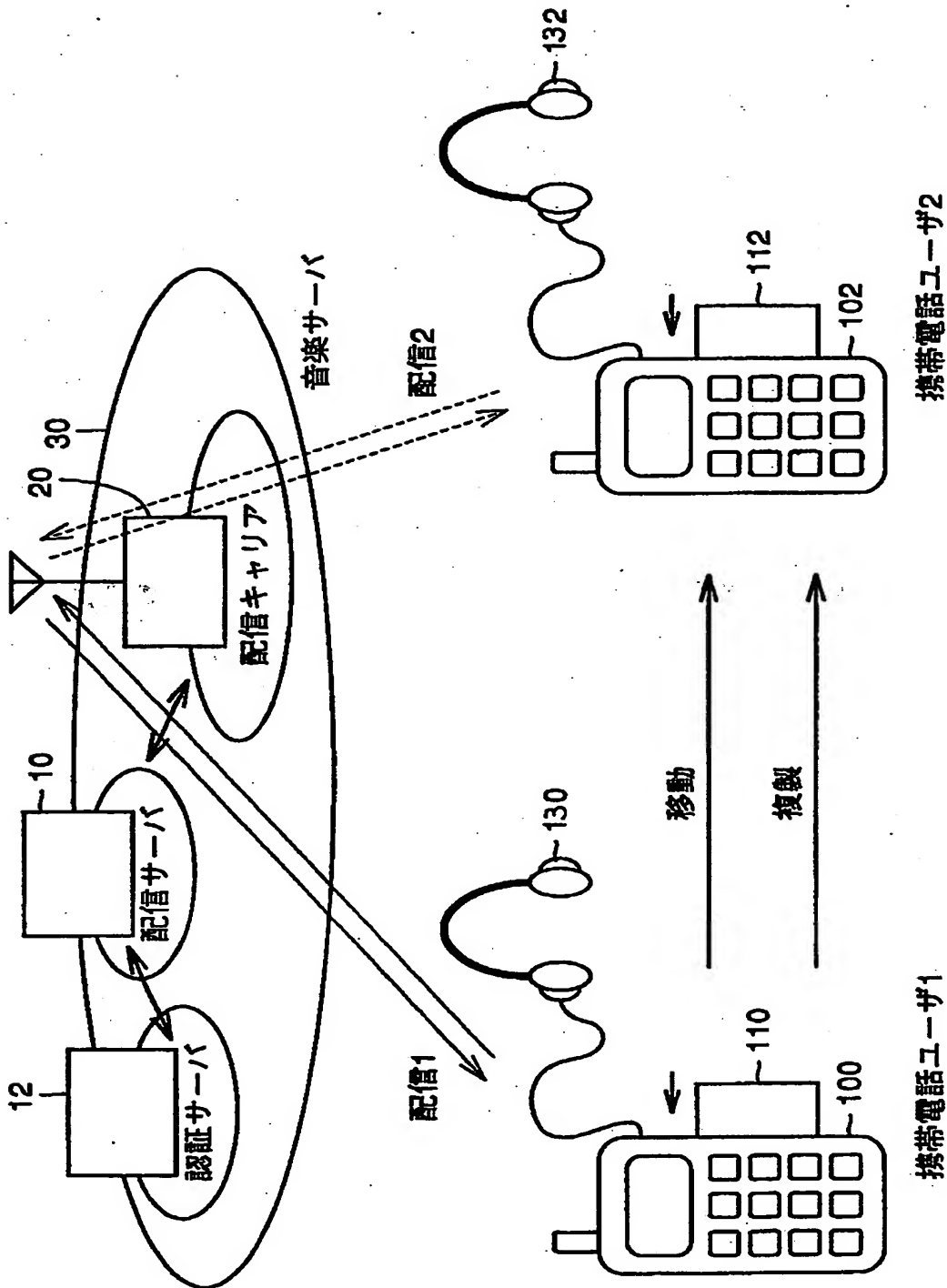
【符号の説明】

10, 11, 12, 13 配信サーバ、20 配信キャリア、30, 31 音楽サーバ、100, 101, 102, 103, 105, 106, 107 携帯電話機、110, 112, 120, 122, 140, 142 メモリカード、130, 132 ヘッドホン、1102 アンテナ、1104 送受信機、1106 コントローラ、1108 タッチキー部、1110 ディスプレイ、1112 音声再生部、1200 メモリインタフェース、1404 復号処理部、1406 暗号化処理部、1408, 1409 切替スイッチ、1410 復号処理部、1412 メモリ、1414 暗号化処理部、1416 復号処理部、1420 コントローラ、1430 暗号化処理部、1432 セッションキー発生部、1434, 1435 切替スイッチ、1502 セッションキー発生部、1504 暗号化処理部、1506 復号処理部、1508 音楽再生部、1510 混合部、1512 デジタルアナログ変換器、1525 [KPp、Crtf] KPmaster保持部、2000, 3000, 3010 コンテンツデータ販売機。

【書類名】

図面

【図 1】

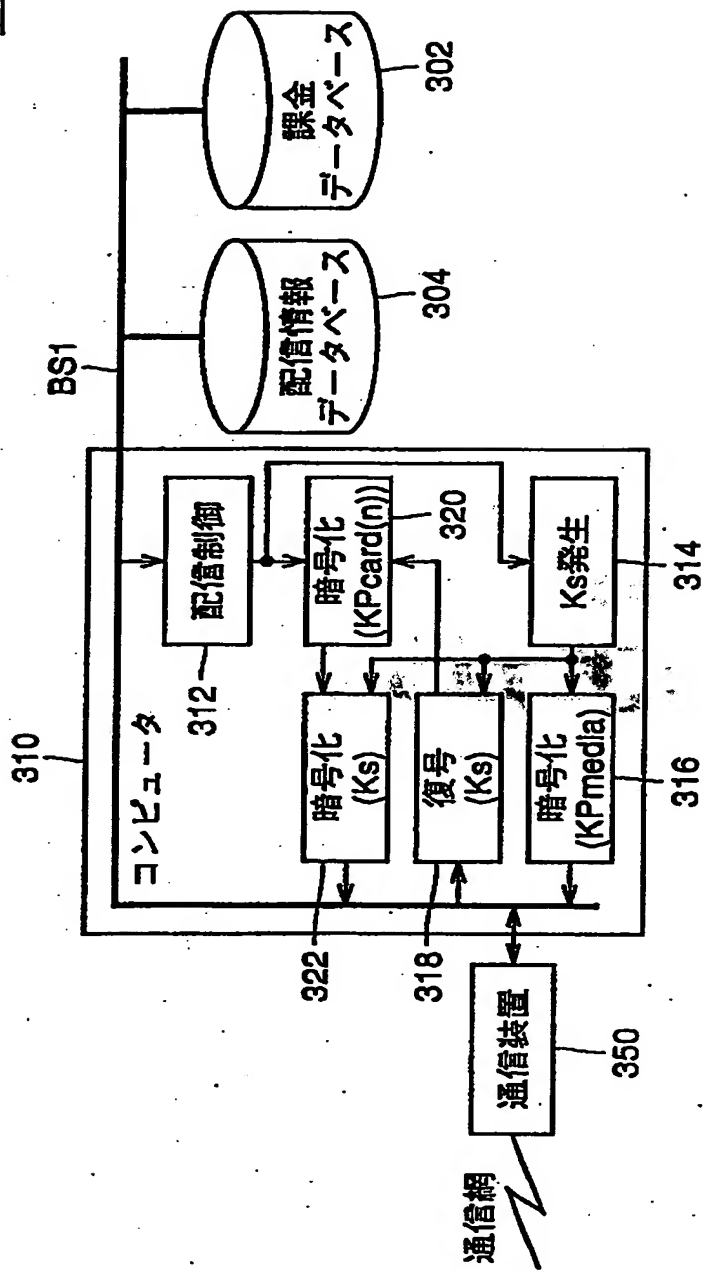


【図 2】

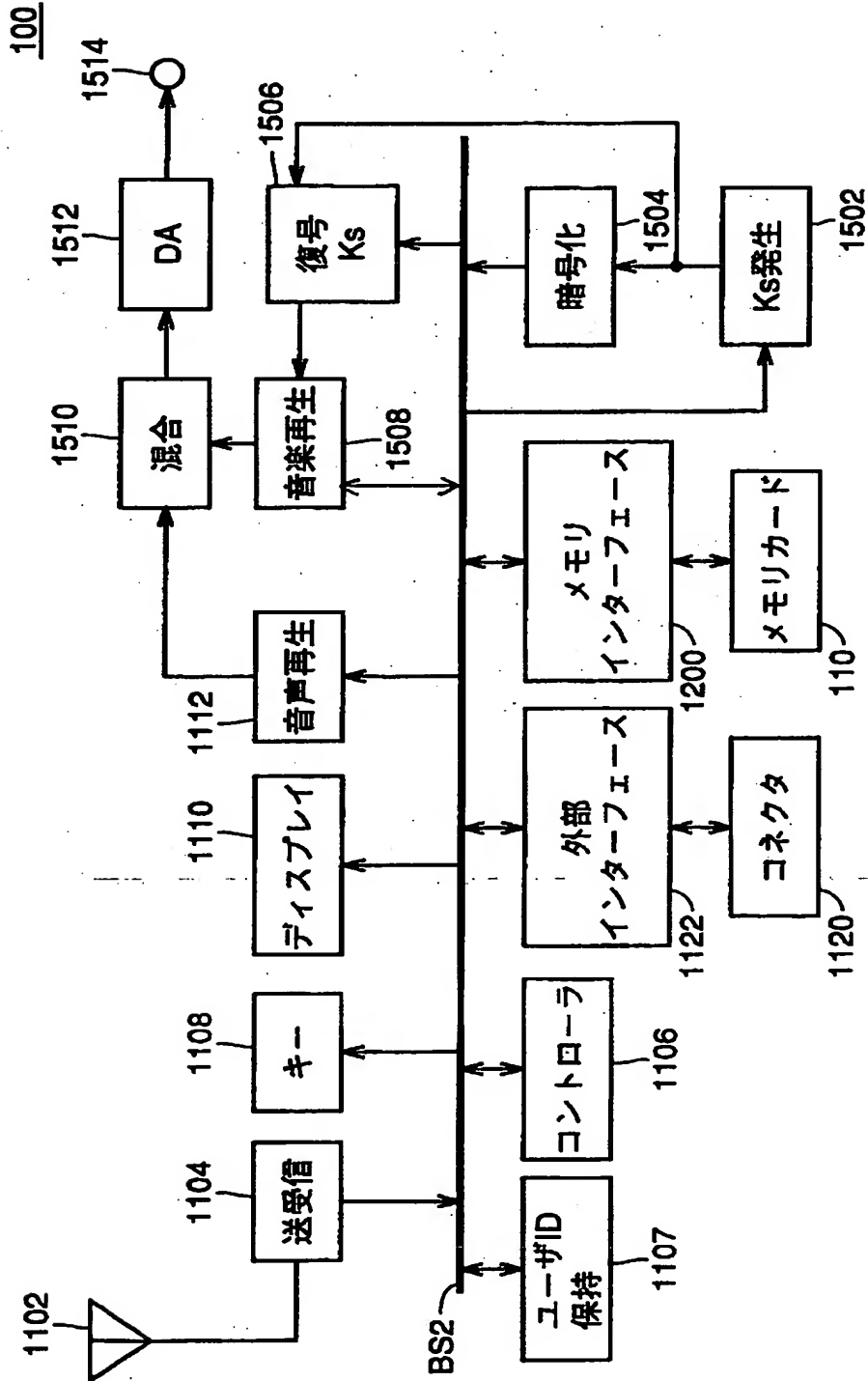
	記号	属性	特性	
			媒体固有	メモリカードの種類ごとに固有な情報を有する
メモリカード内 管理の鍵	Kmedia(n)	秘密復号鍵		メモリカード毎に異なる
	Kcard(n)	秘密復号鍵		Kcard(n)と対を成す。
	KPcard(n)	公開暗号化鍵		KPcard(n)により暗号化されたデータは、Kcard(n)で復号可能
メモリカード外 管理の鍵	KPmedia(n)	公開暗号化鍵	媒体固有	Kmediaと対を成す。 KPmediaにより暗号化されたデータは、Kmediaで復号可能。
	Ks	共通鍵	セッション 固有	通信毎 (例：アクセス毎) に発生。 配信サーバ、携帯電話機にて管理
配信データ	Kc	共通鍵	ライセン スキー	暗号化コンテンツデータの復号鍵
	License-ID	再生に関する 情報		例：曲目の特定情報 再生回数の制限情報
	User-ID	受信者を識別 する情報		例：電話番号
	Dc	コンテンツ データ		例：音楽
	[Dc]Kc	暗号化コン テンツデータ		共通鍵Kcにより暗号化されたコンテンツデータ

【図 3】

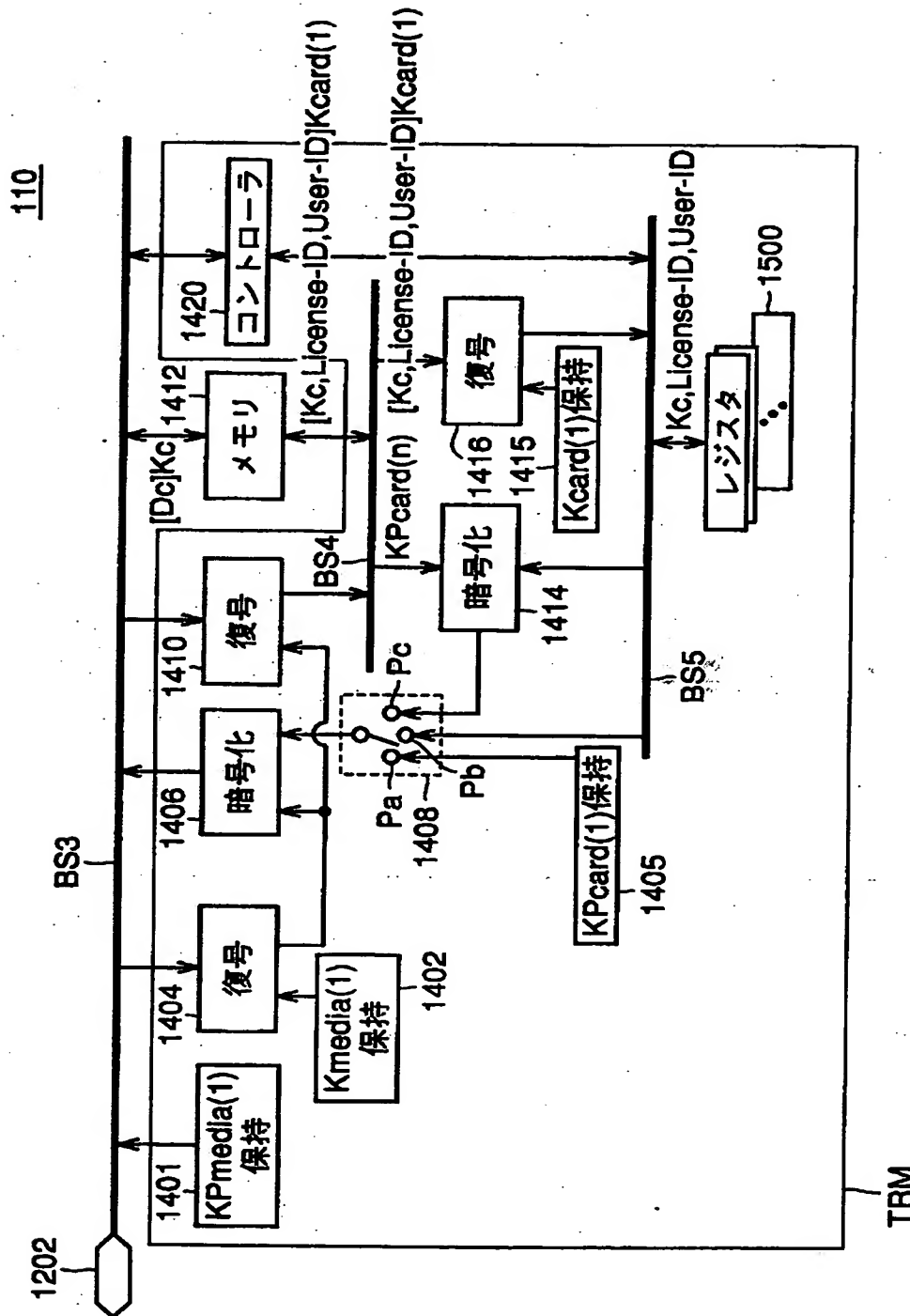
10



【図 4】

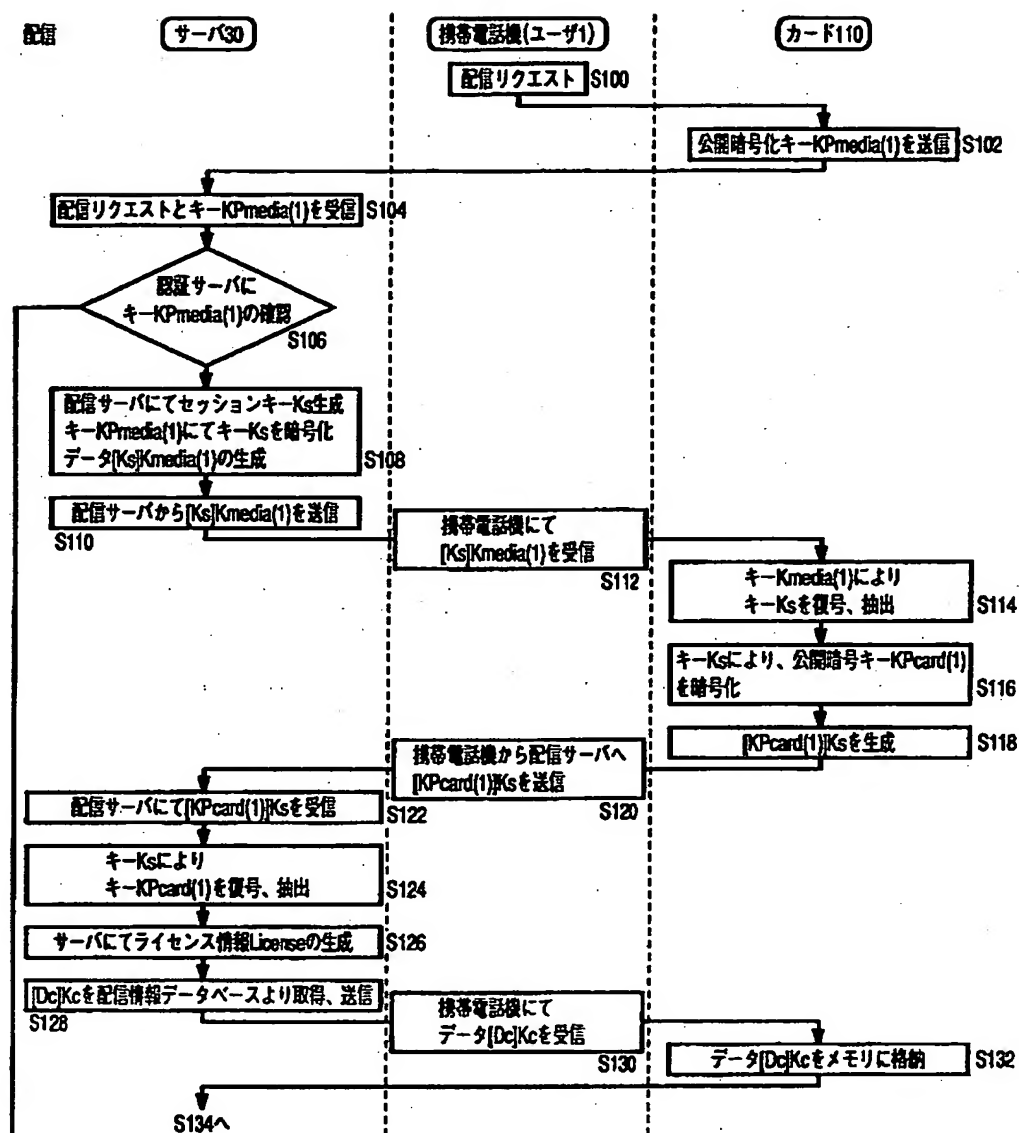


【図 5】

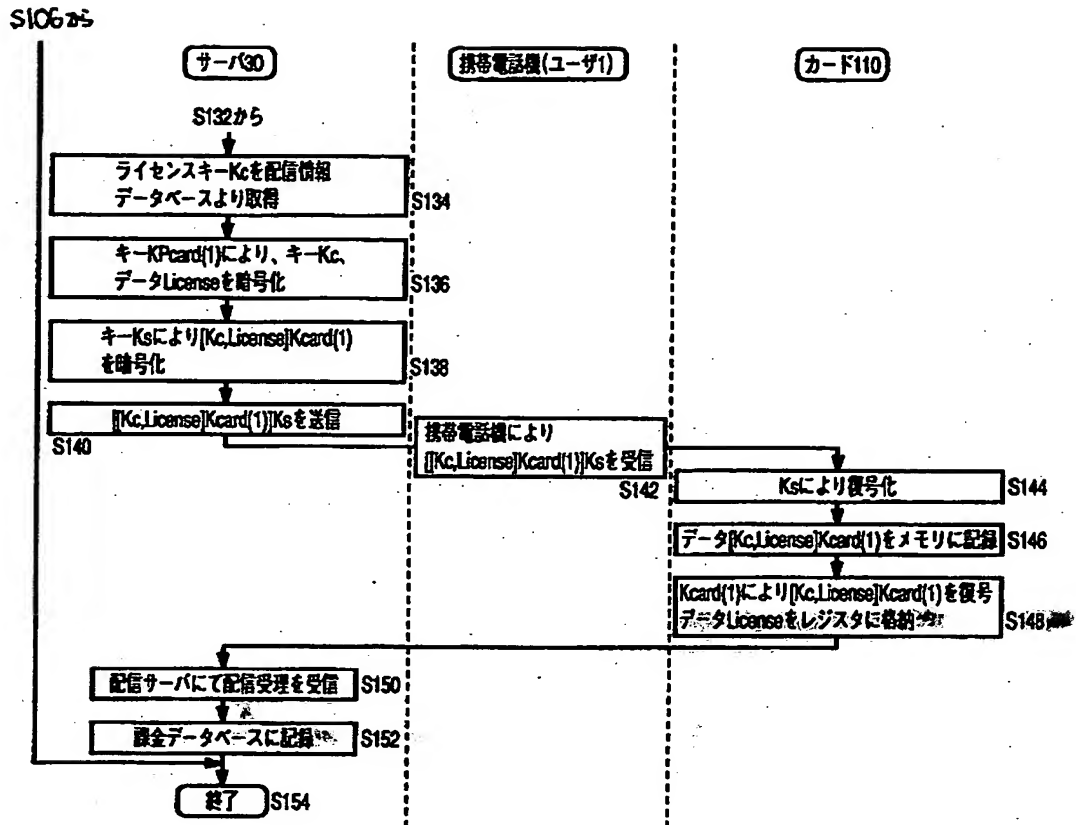




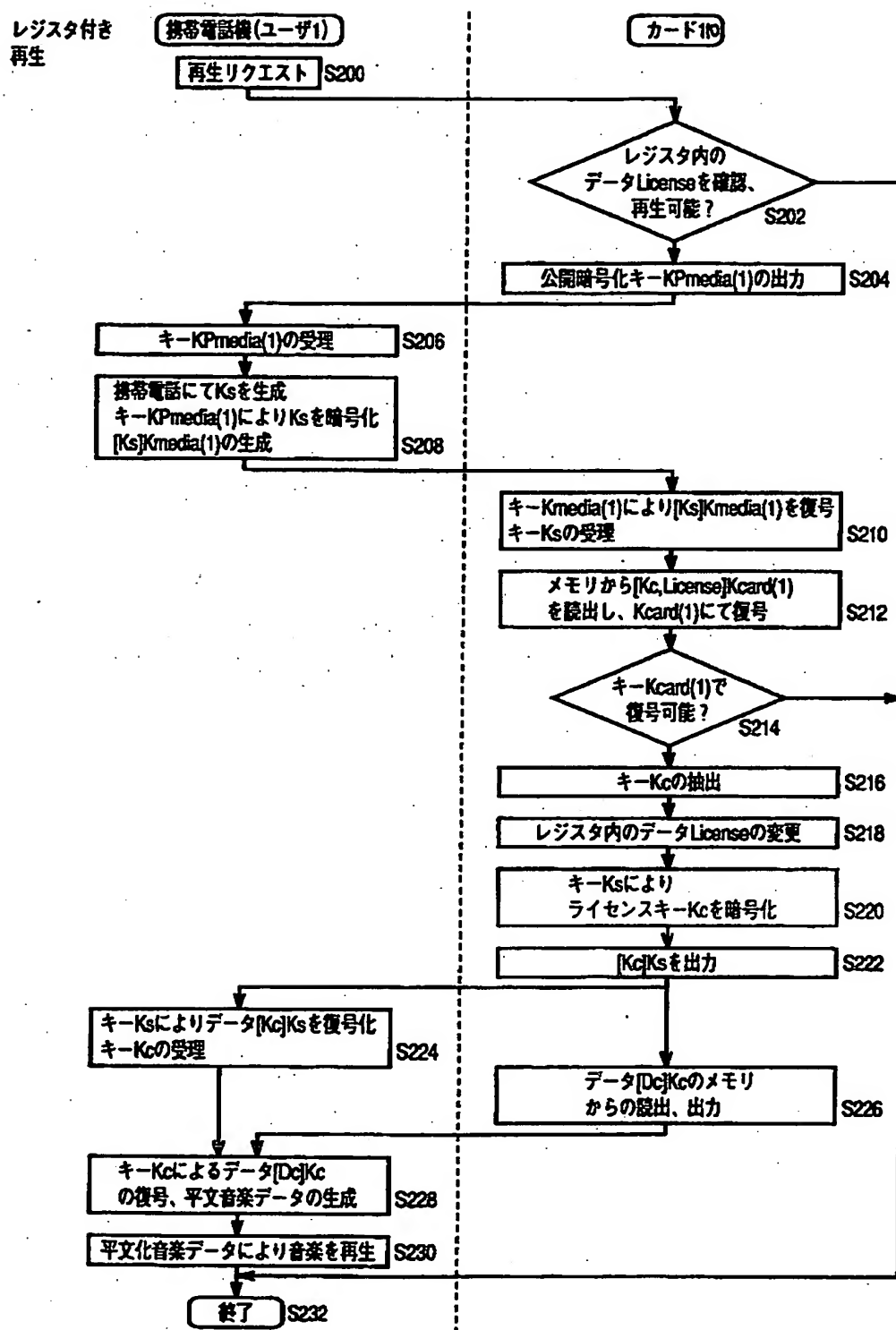
【図 6】



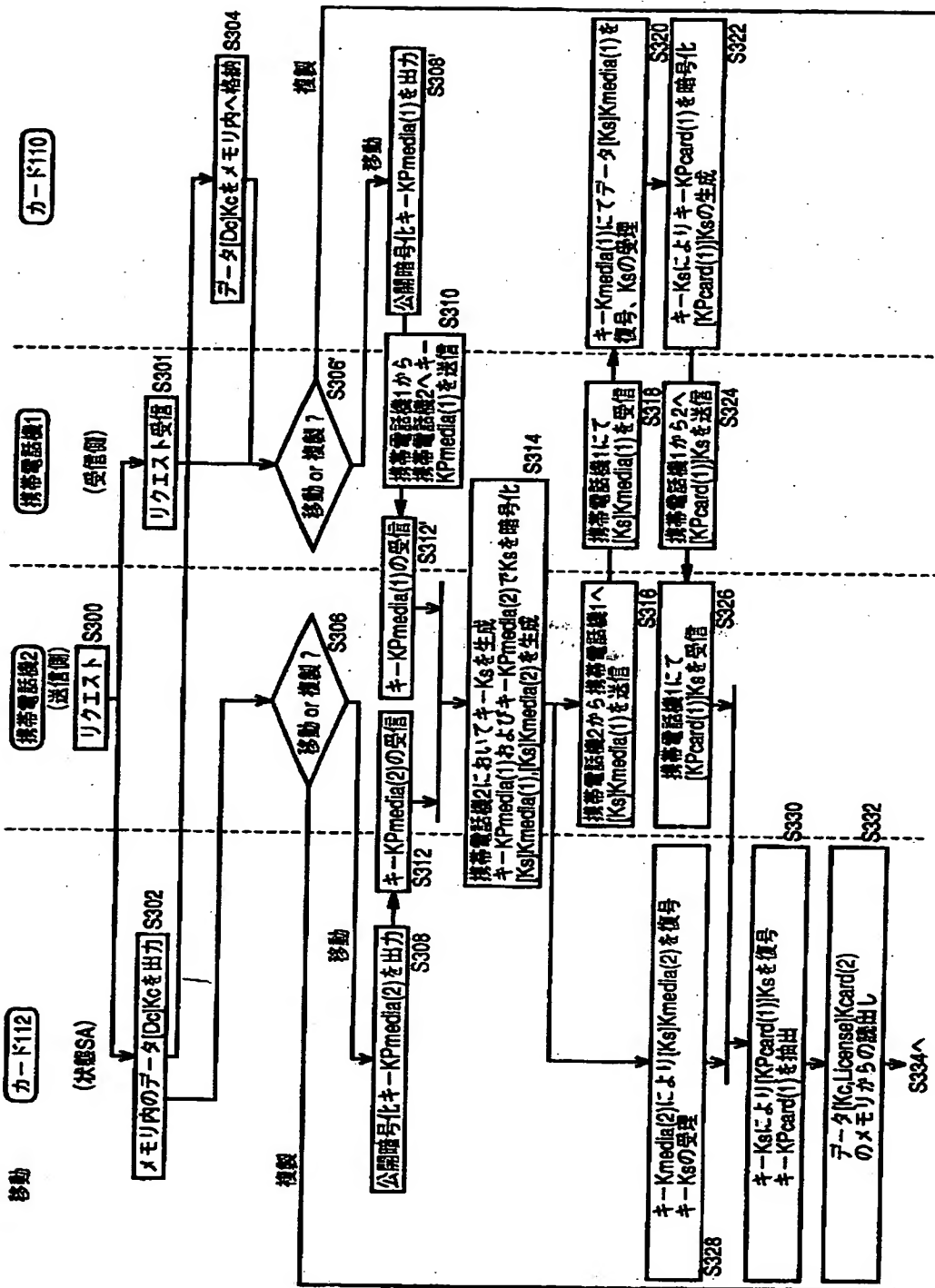
【図 7】



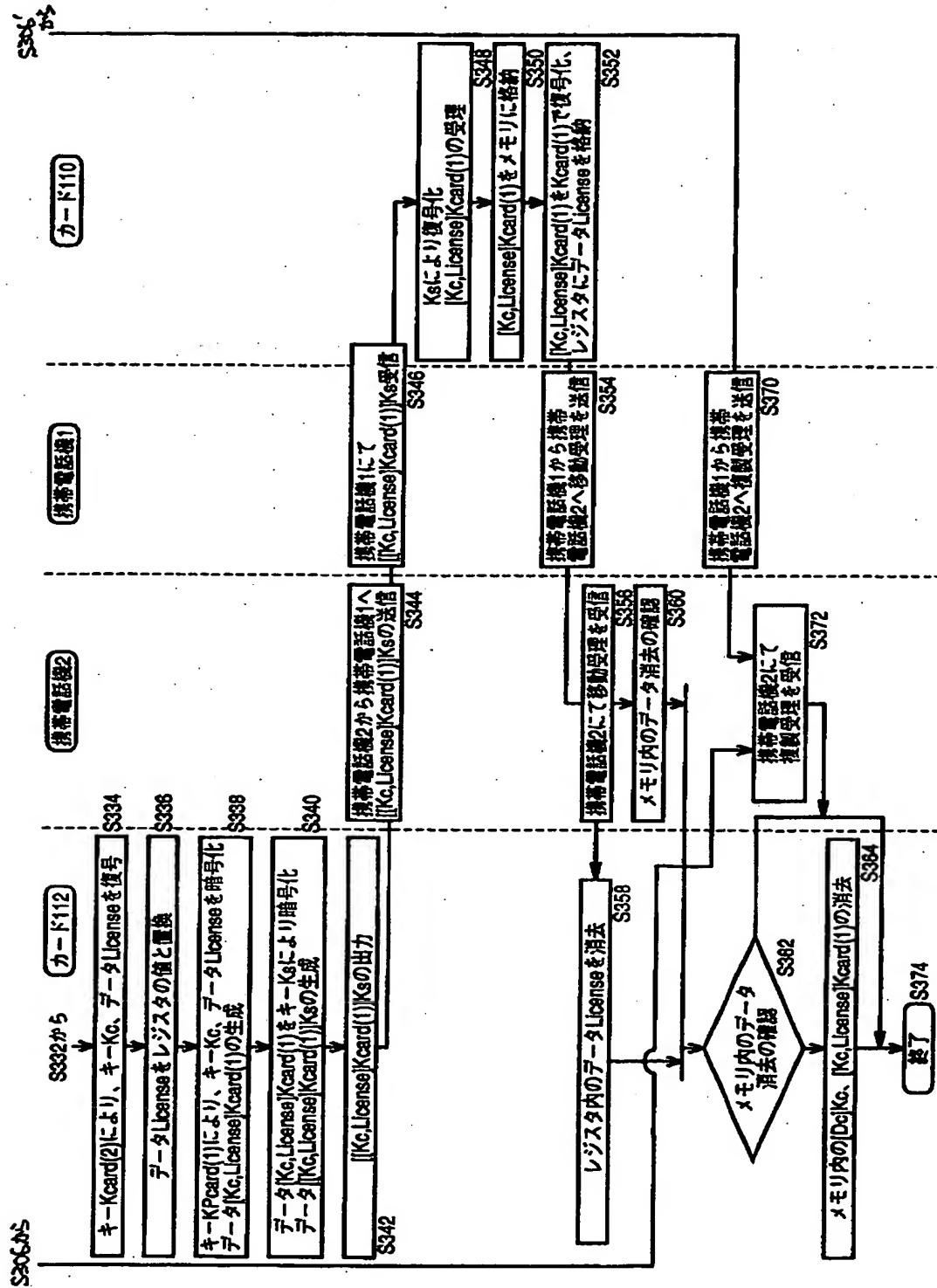
【図 8】



【図9】

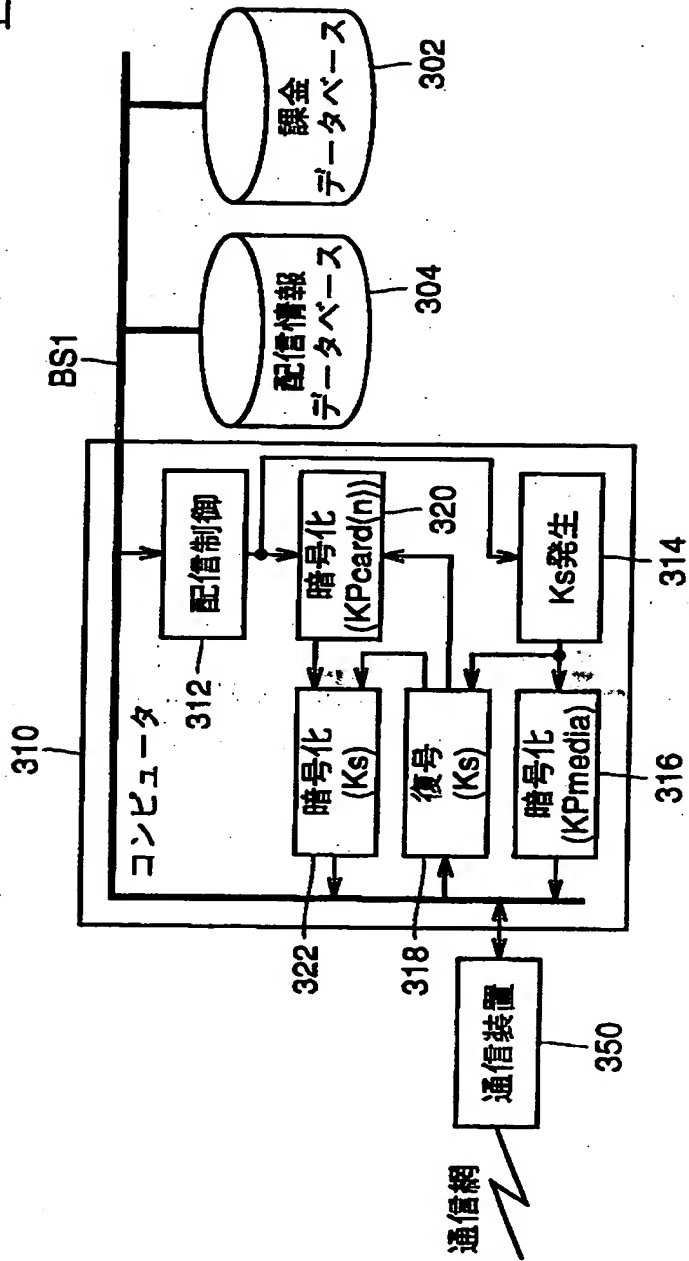


【図 10】

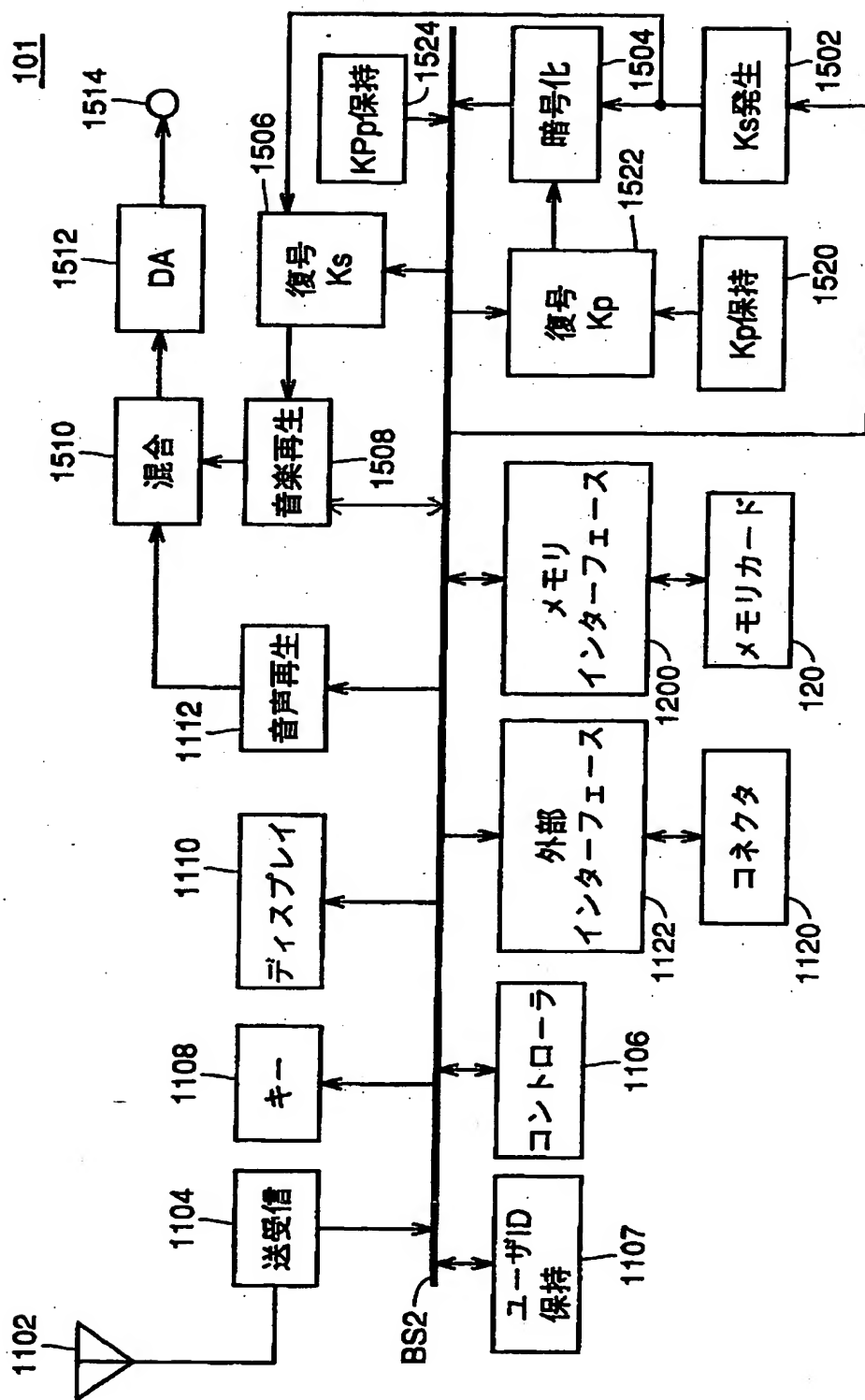


【図 1 1】

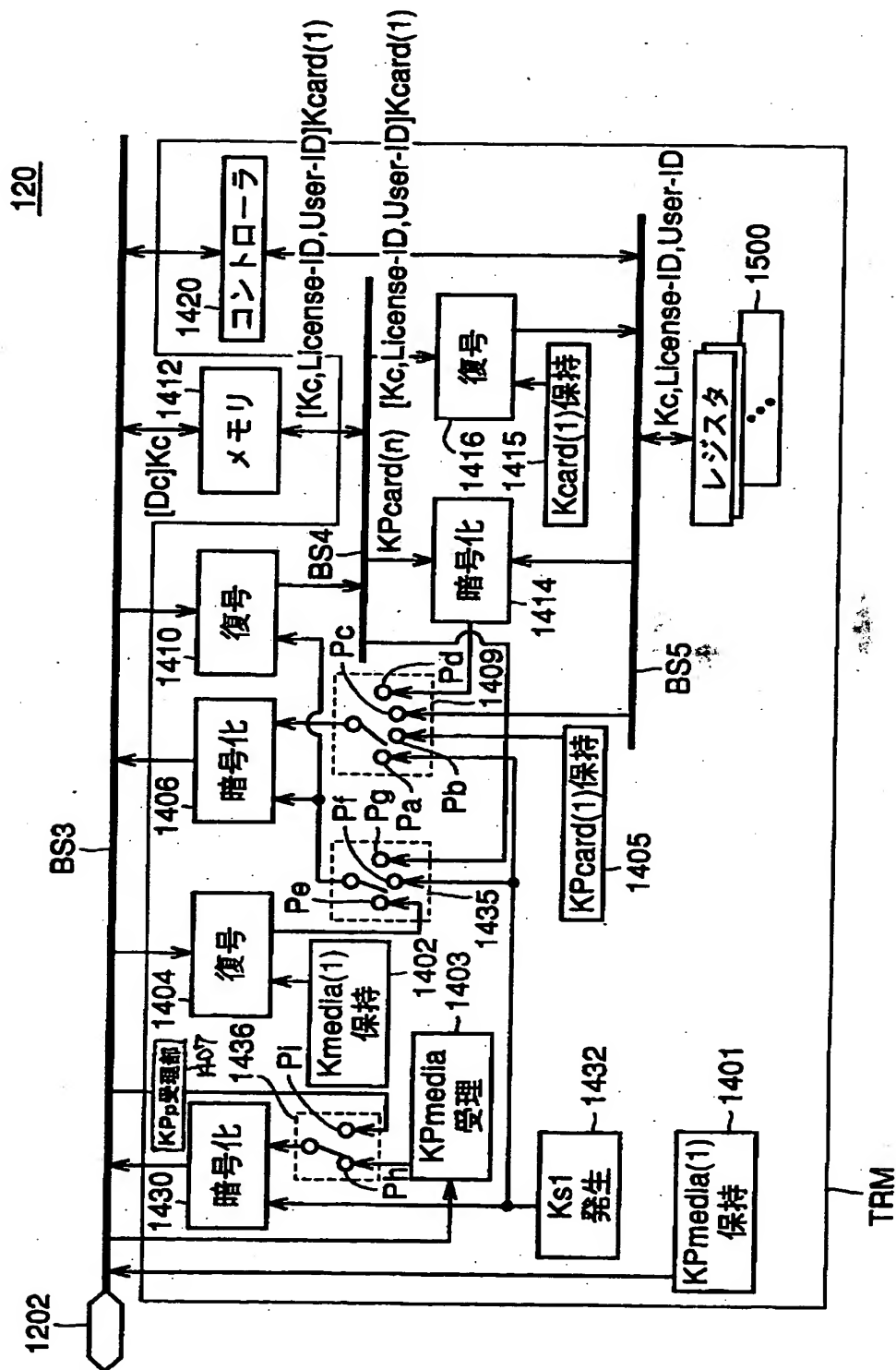
11



【図 1 2】

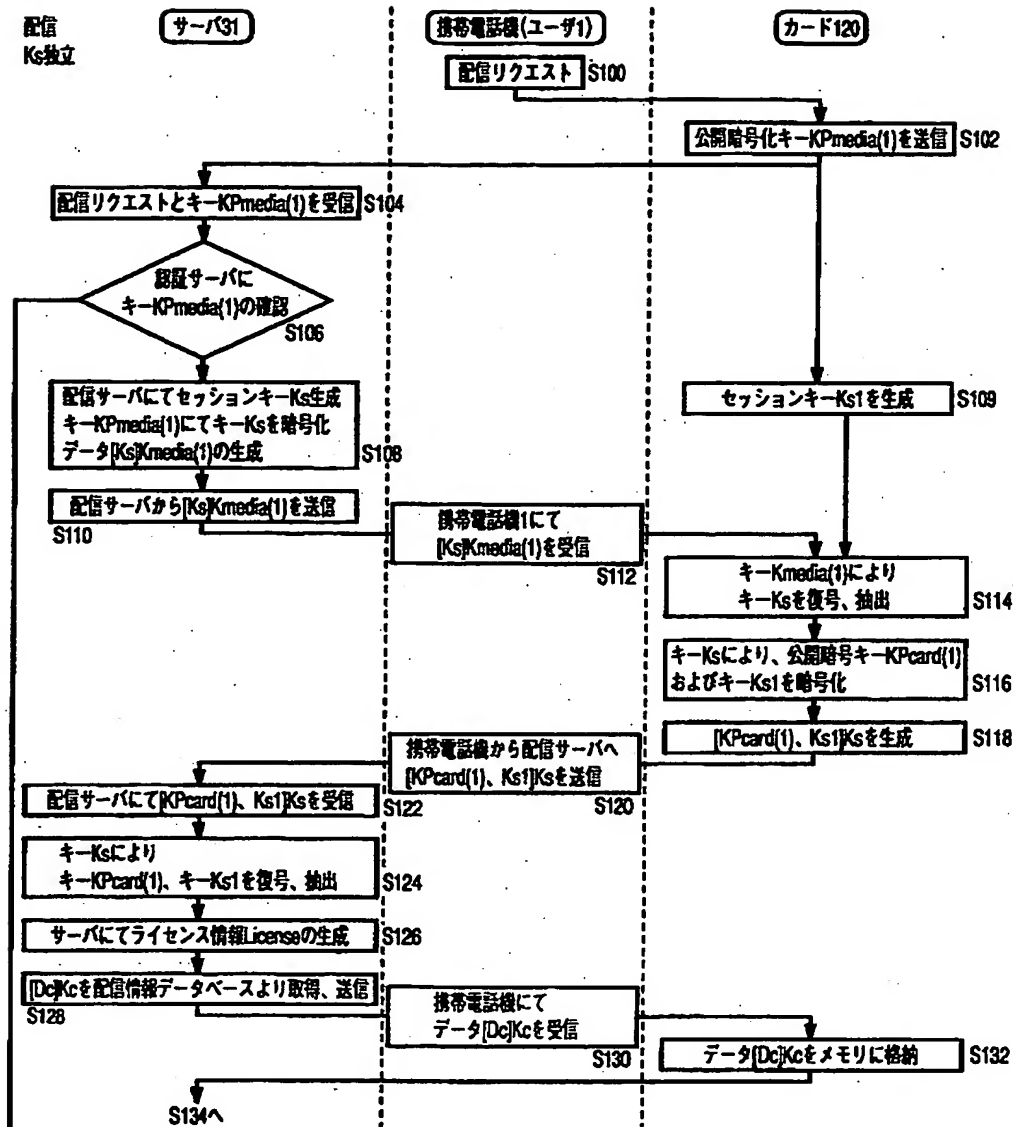


【図 13】

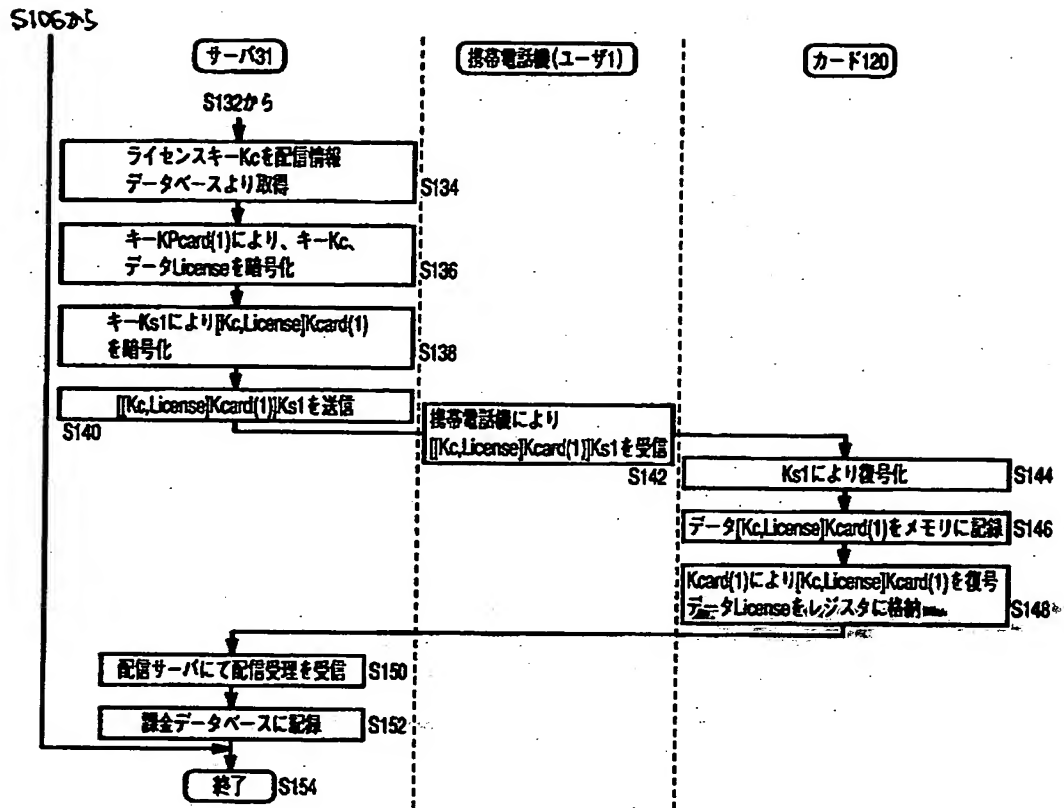




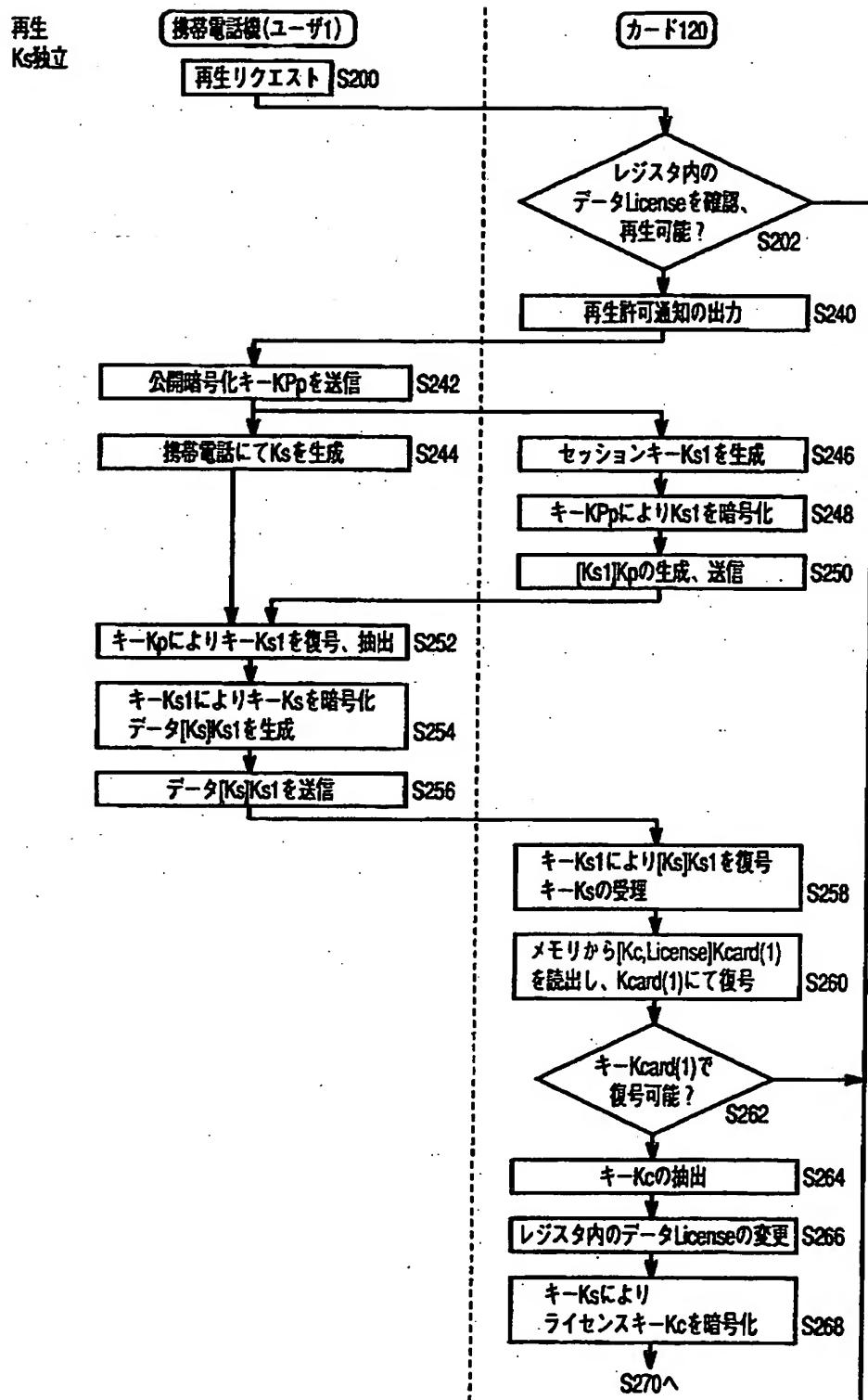
【図 1 4】



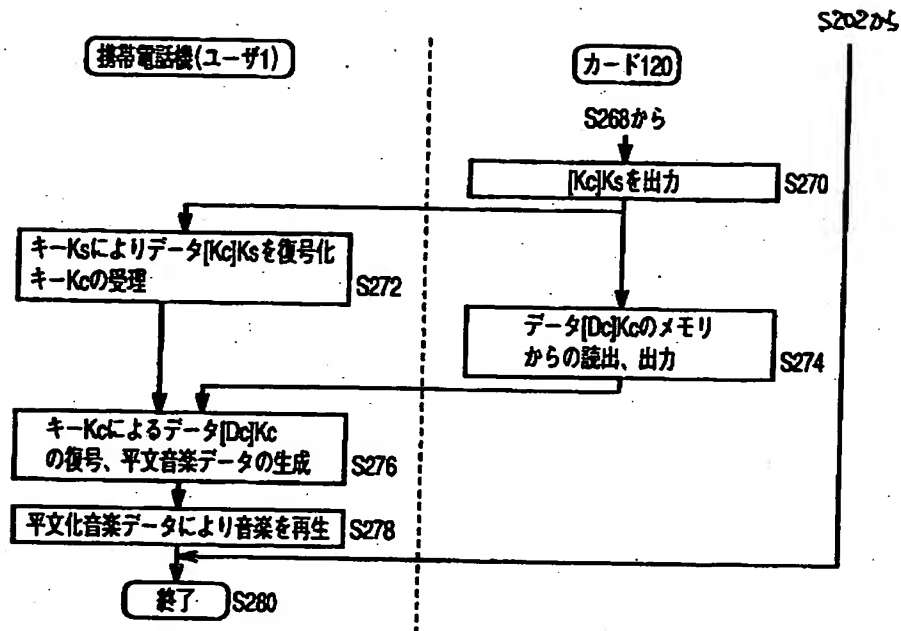
【図 1 5】



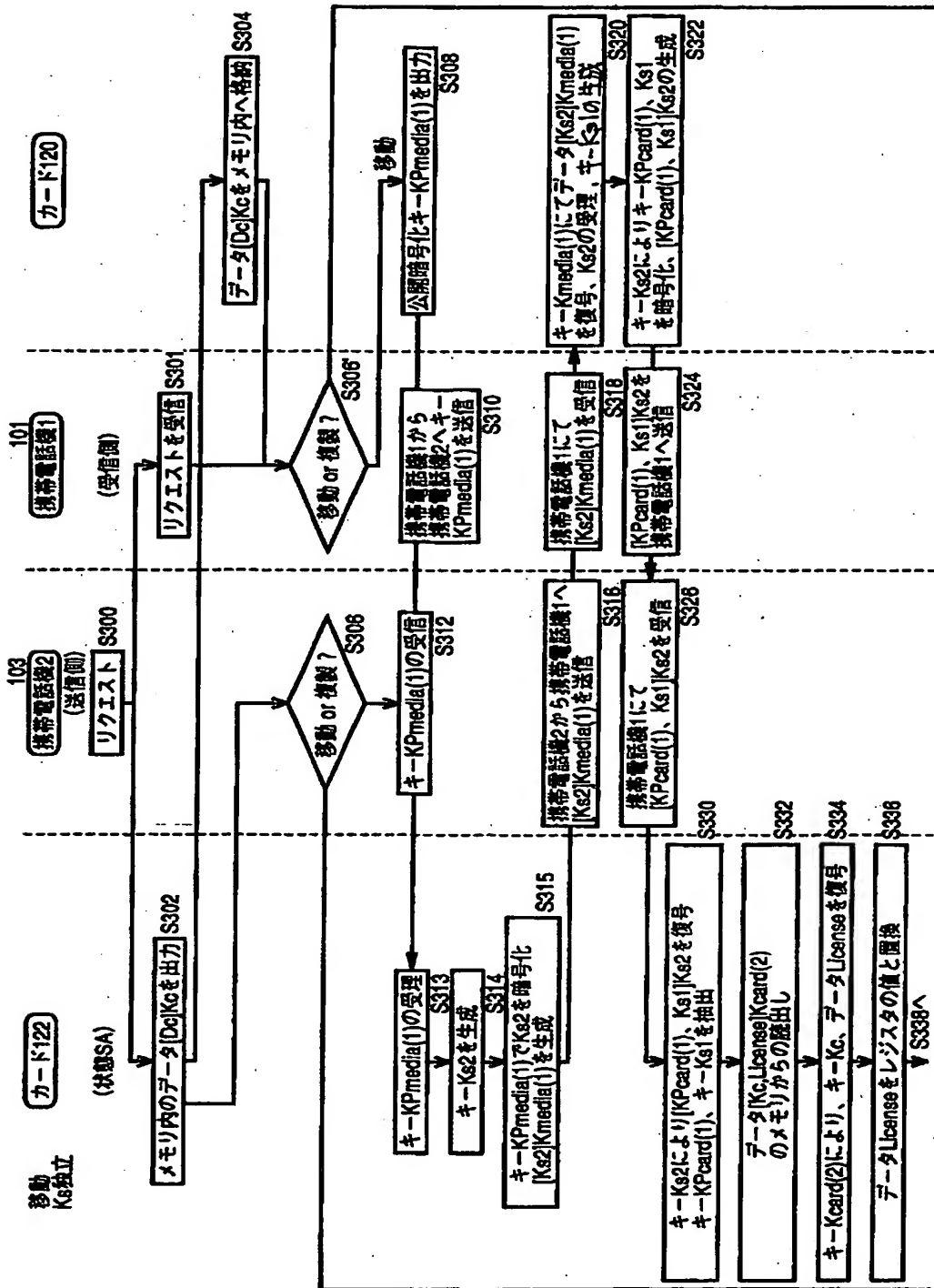
【図 16】



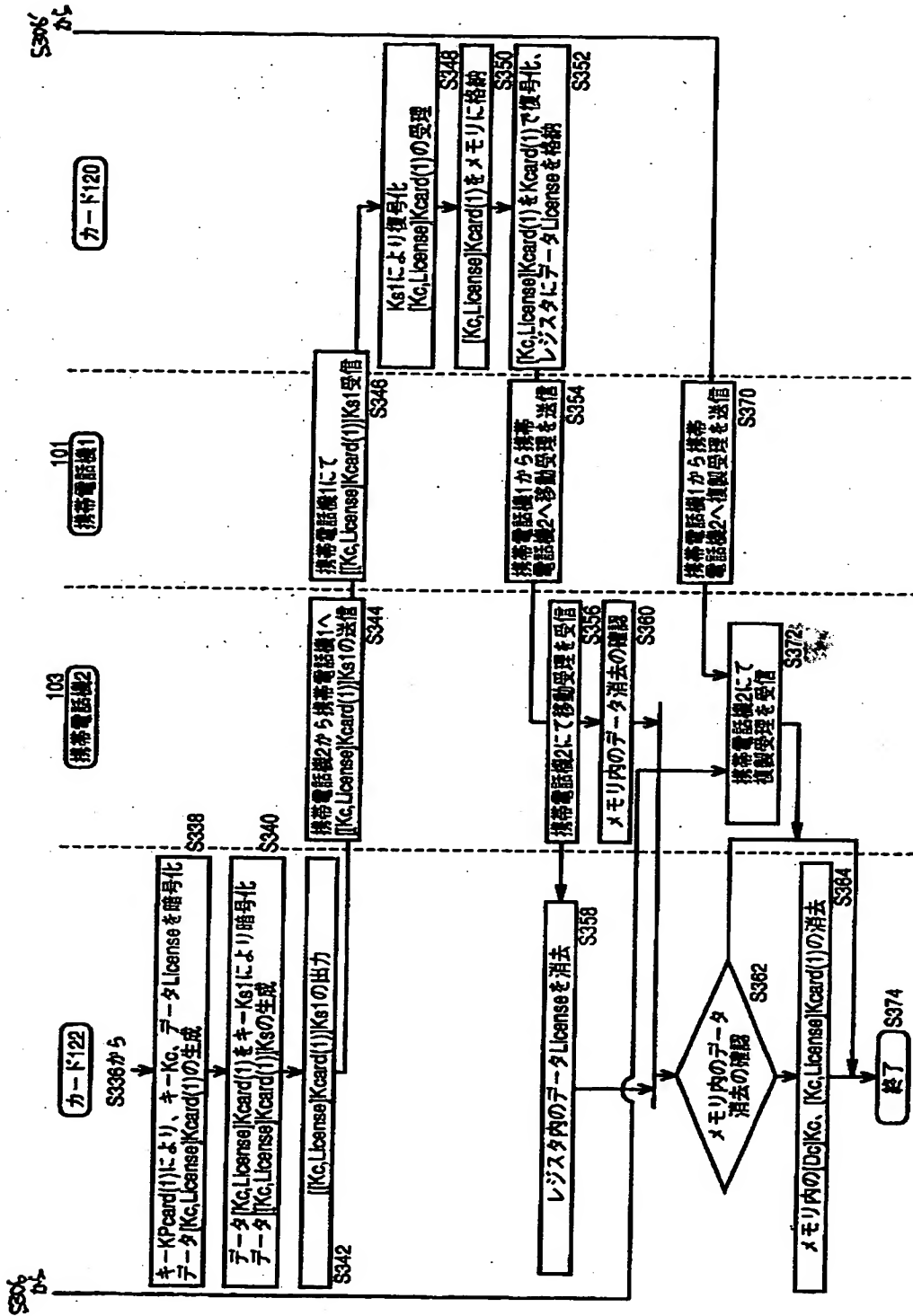
【図 1 7】



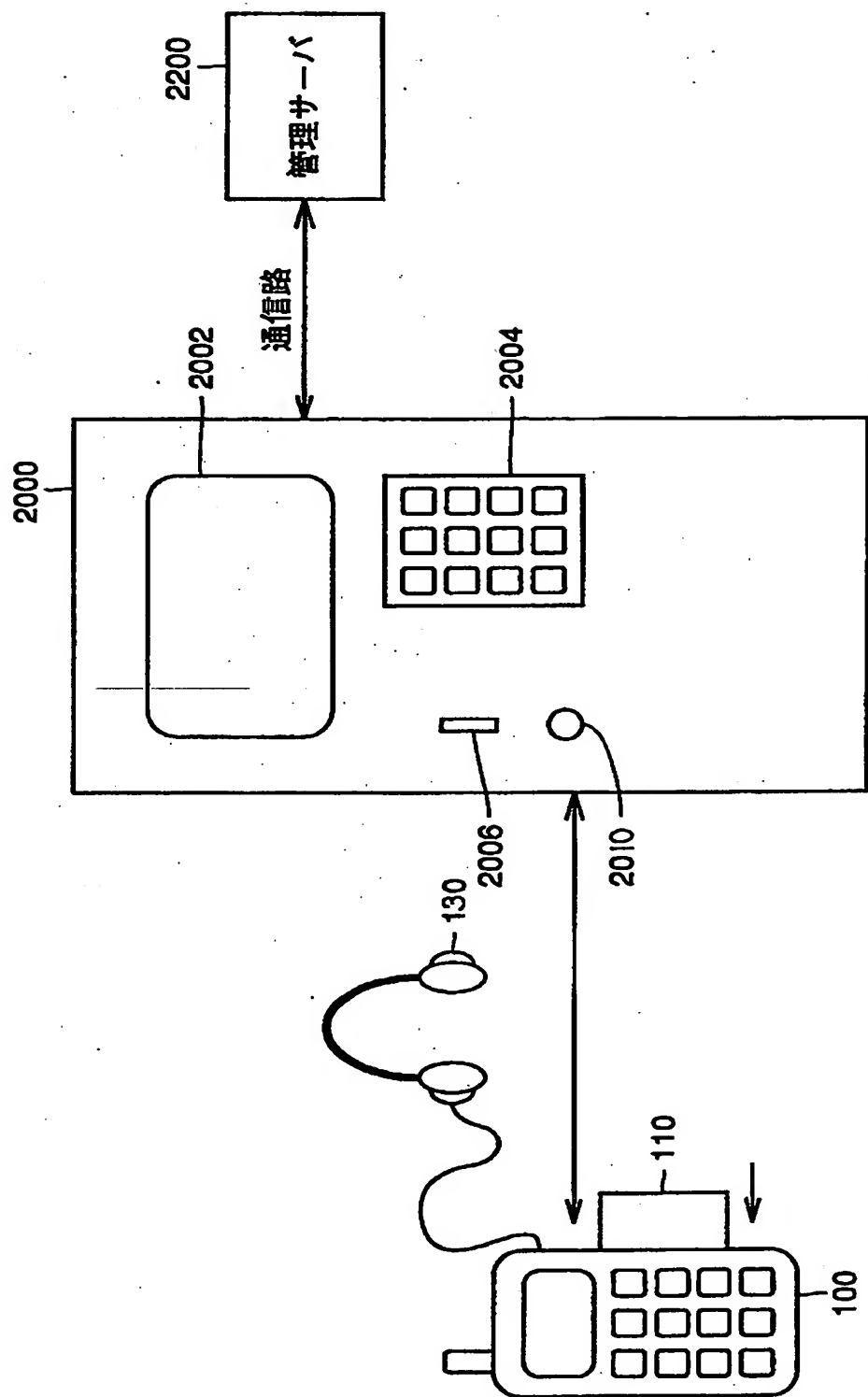
【圖 18】



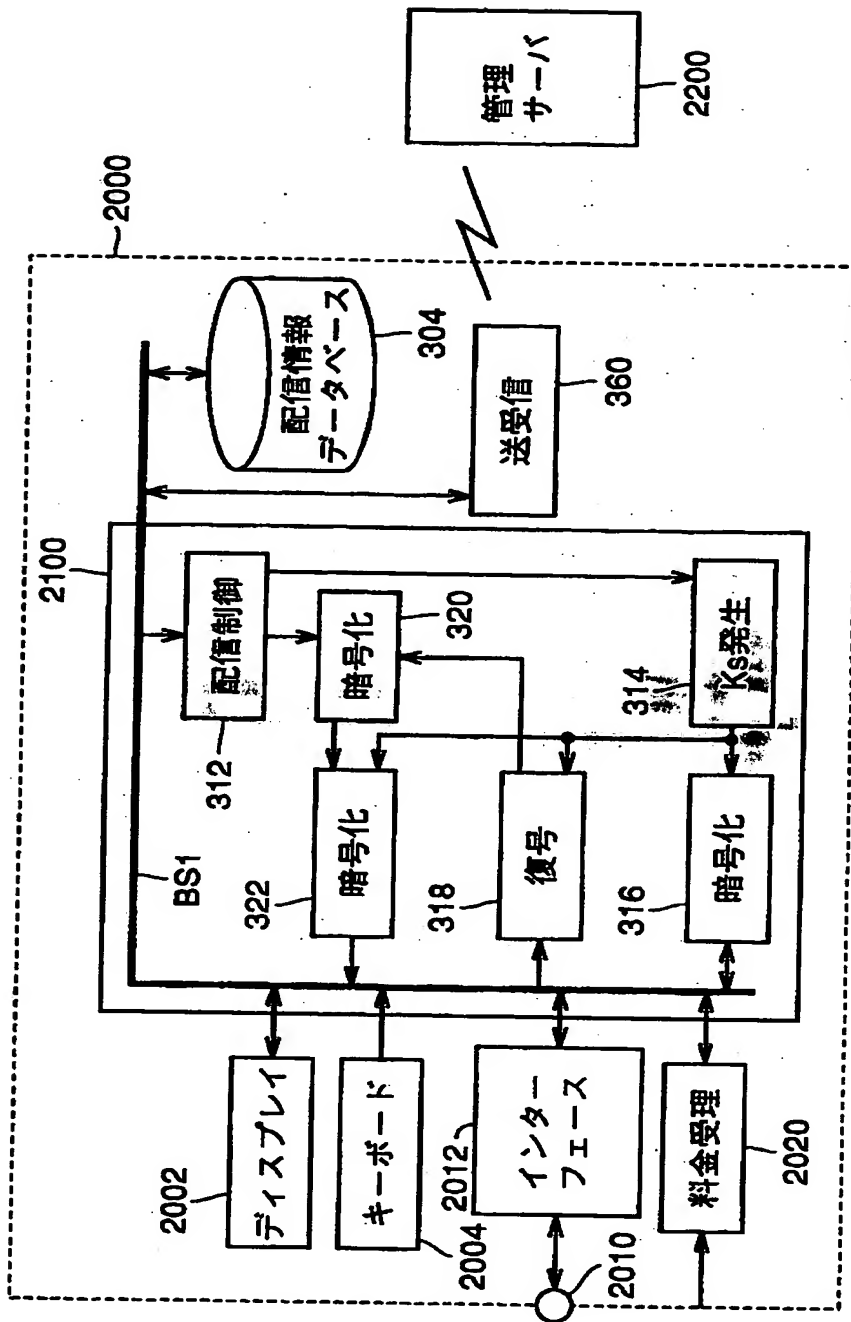
【図 1 9】



【図 2 0】

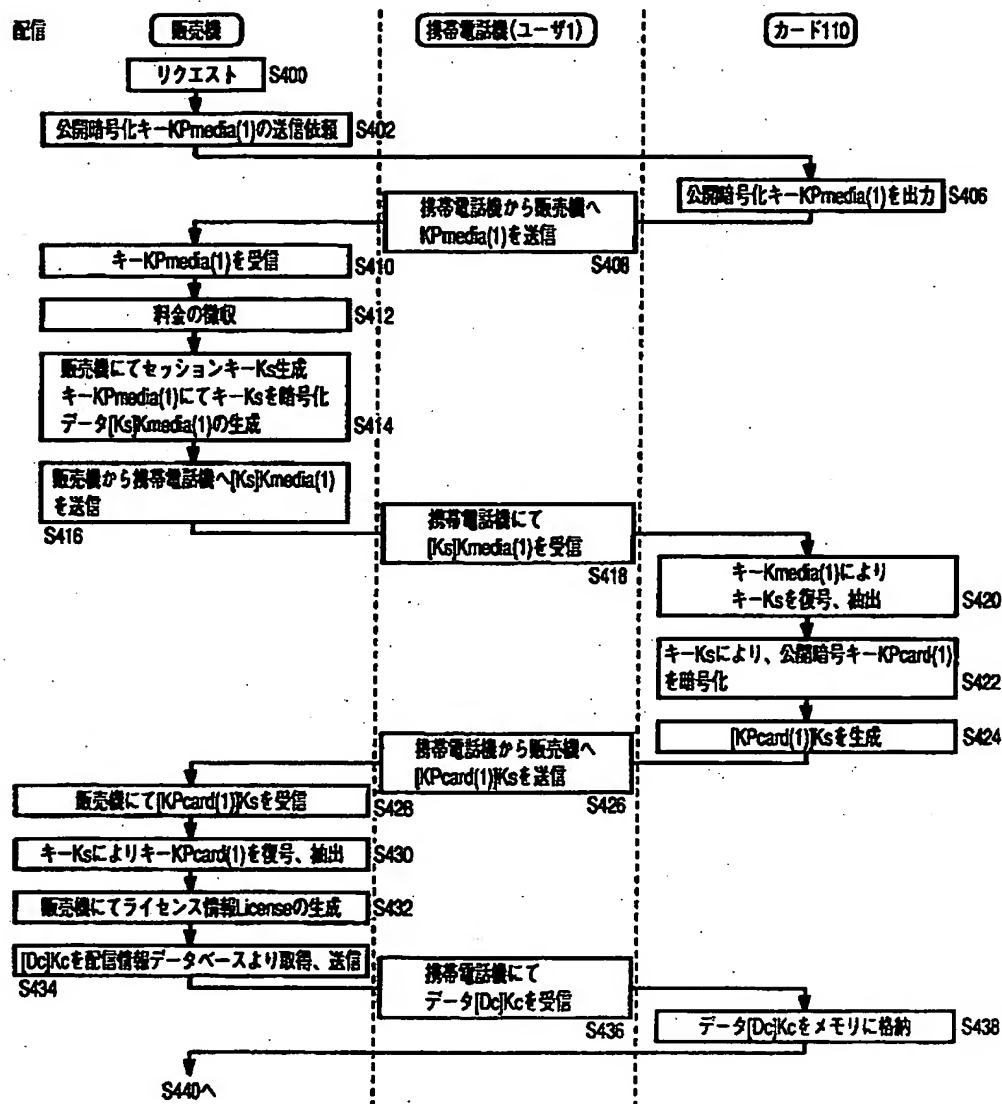


【図 2 1】

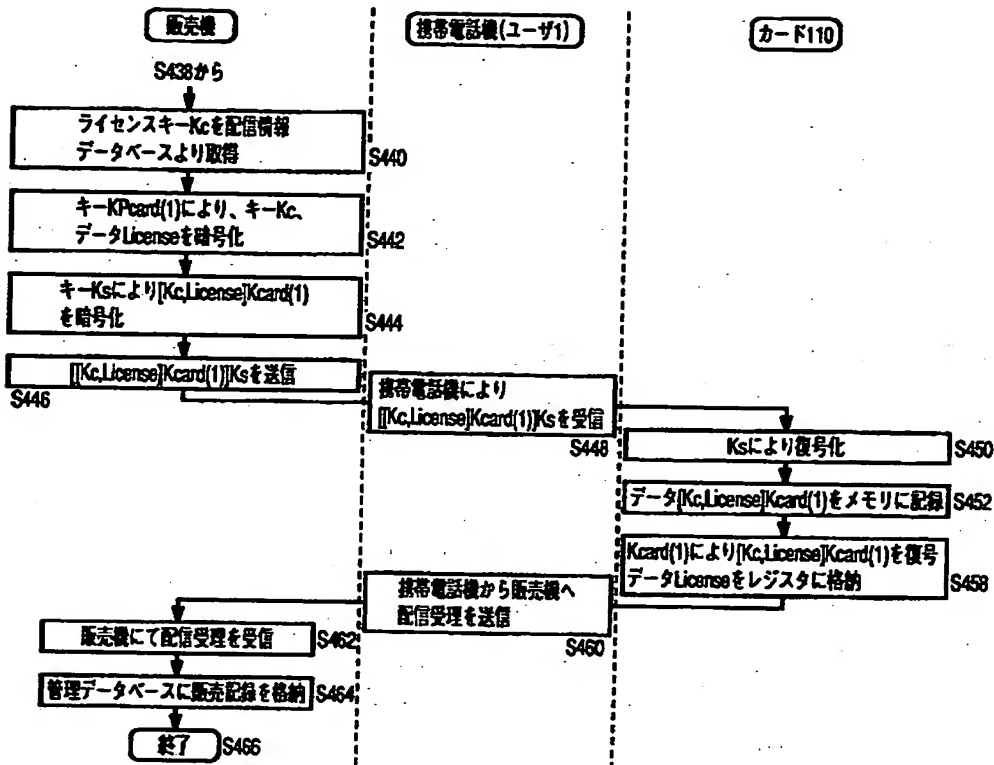




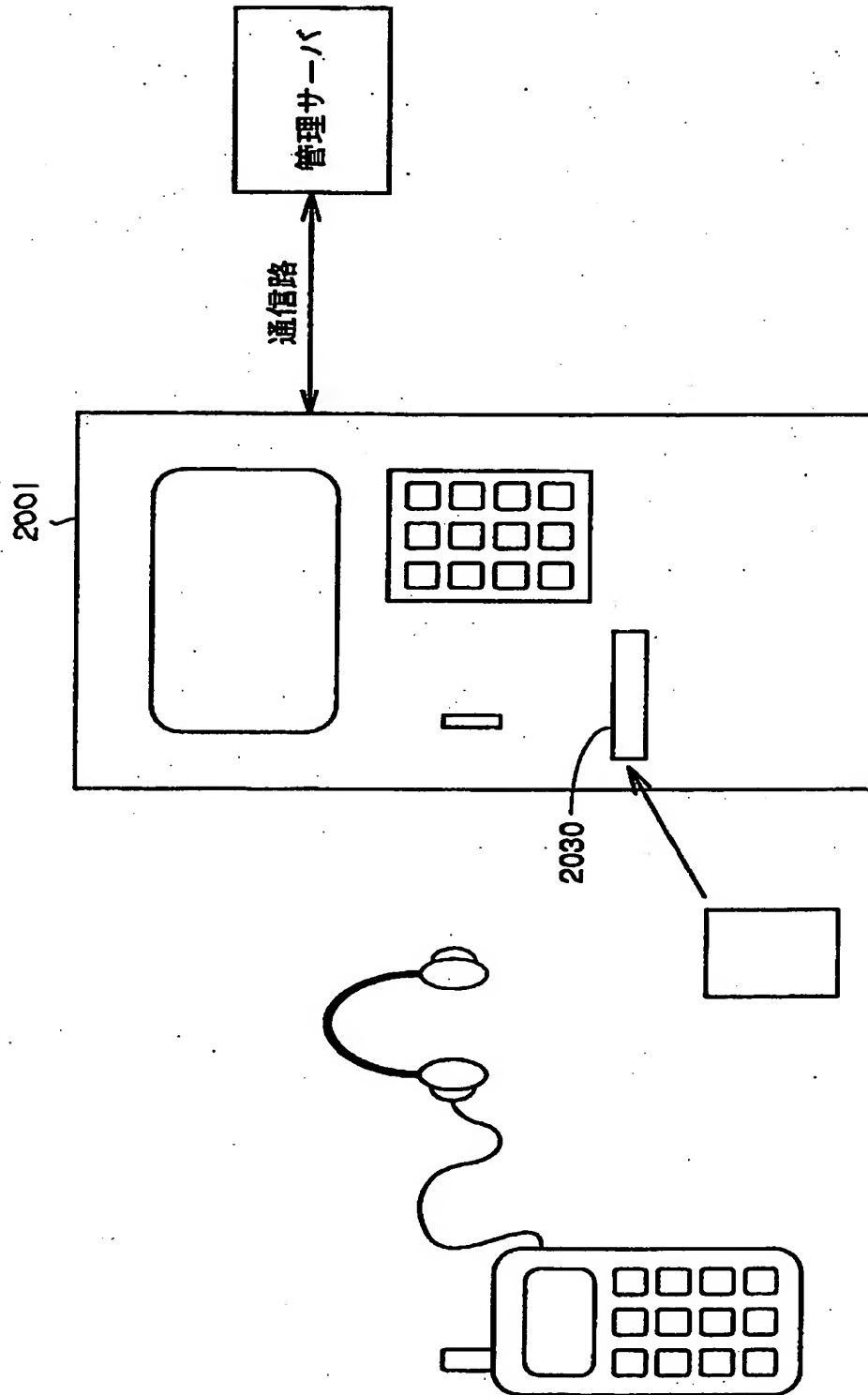
【図 2 2】



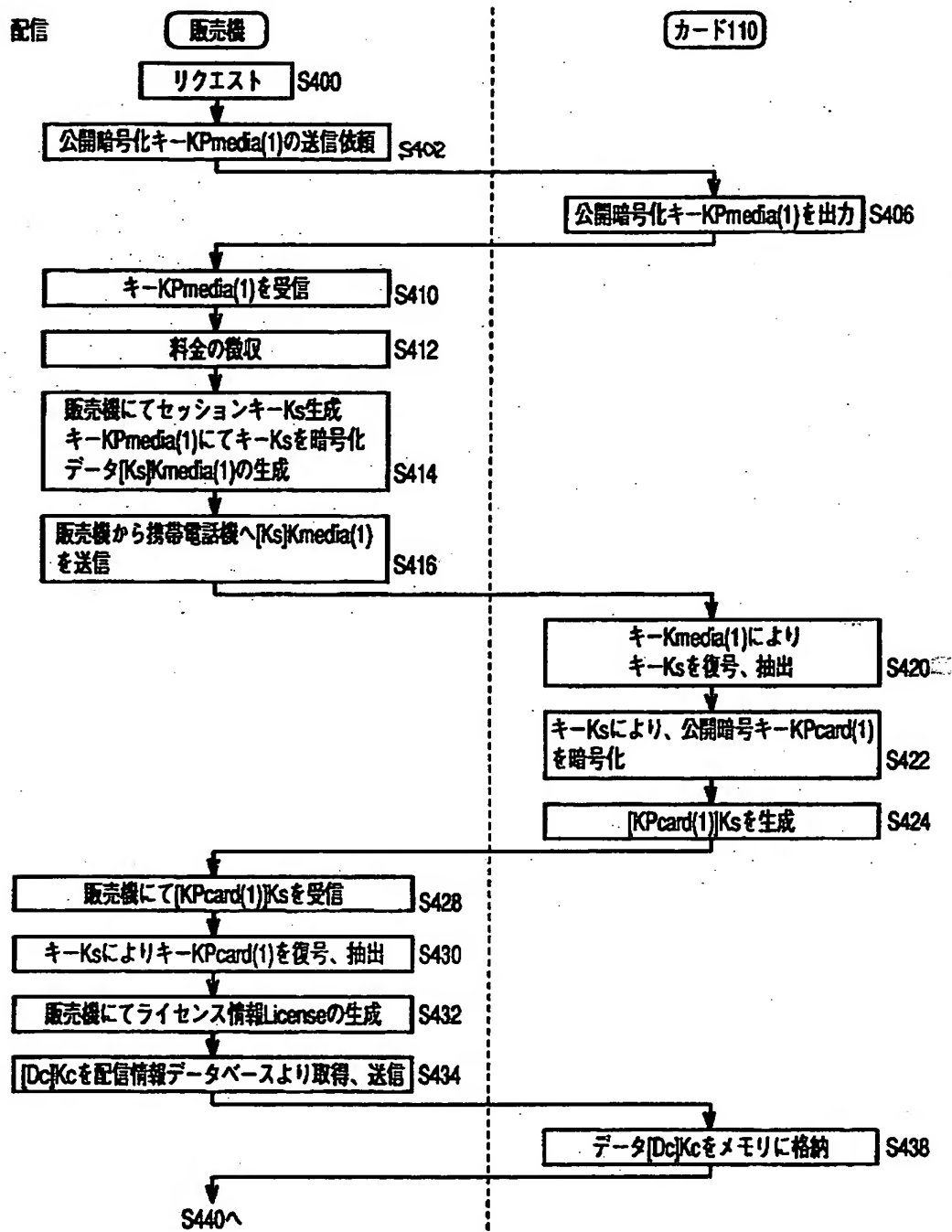
【図 23】



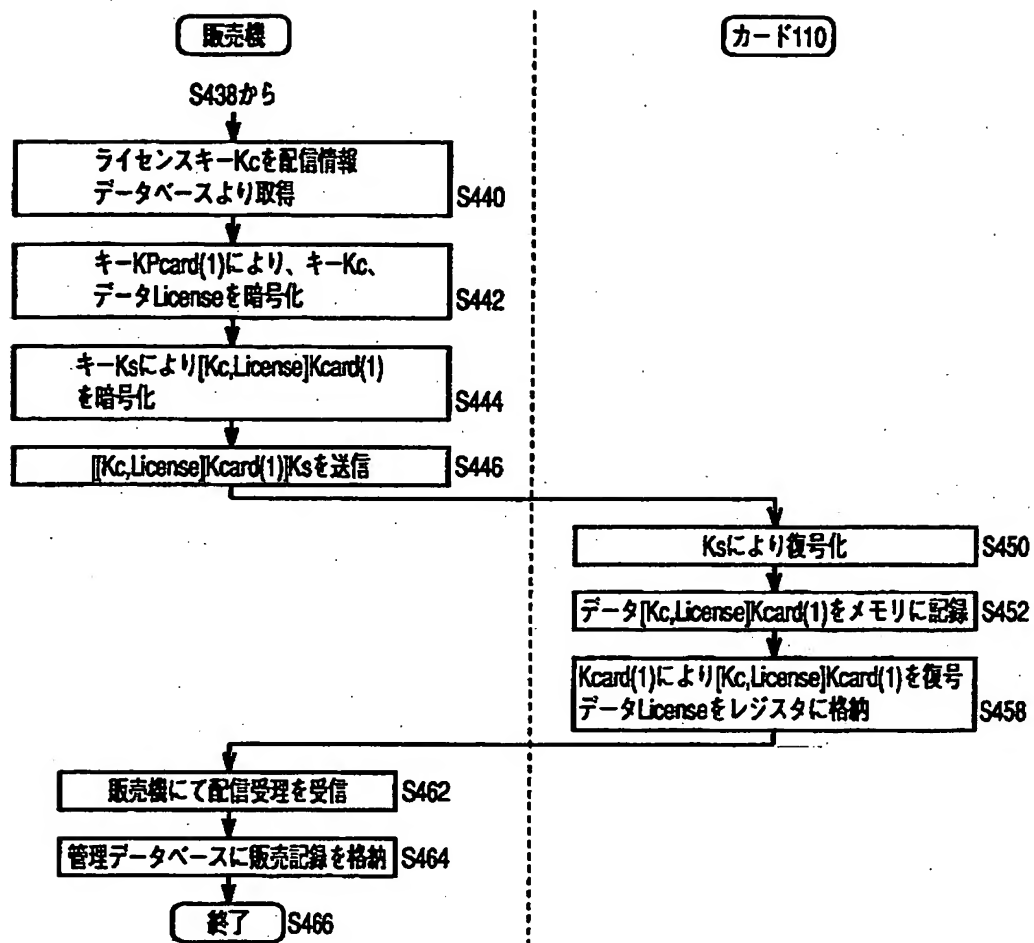
【図 2 4】



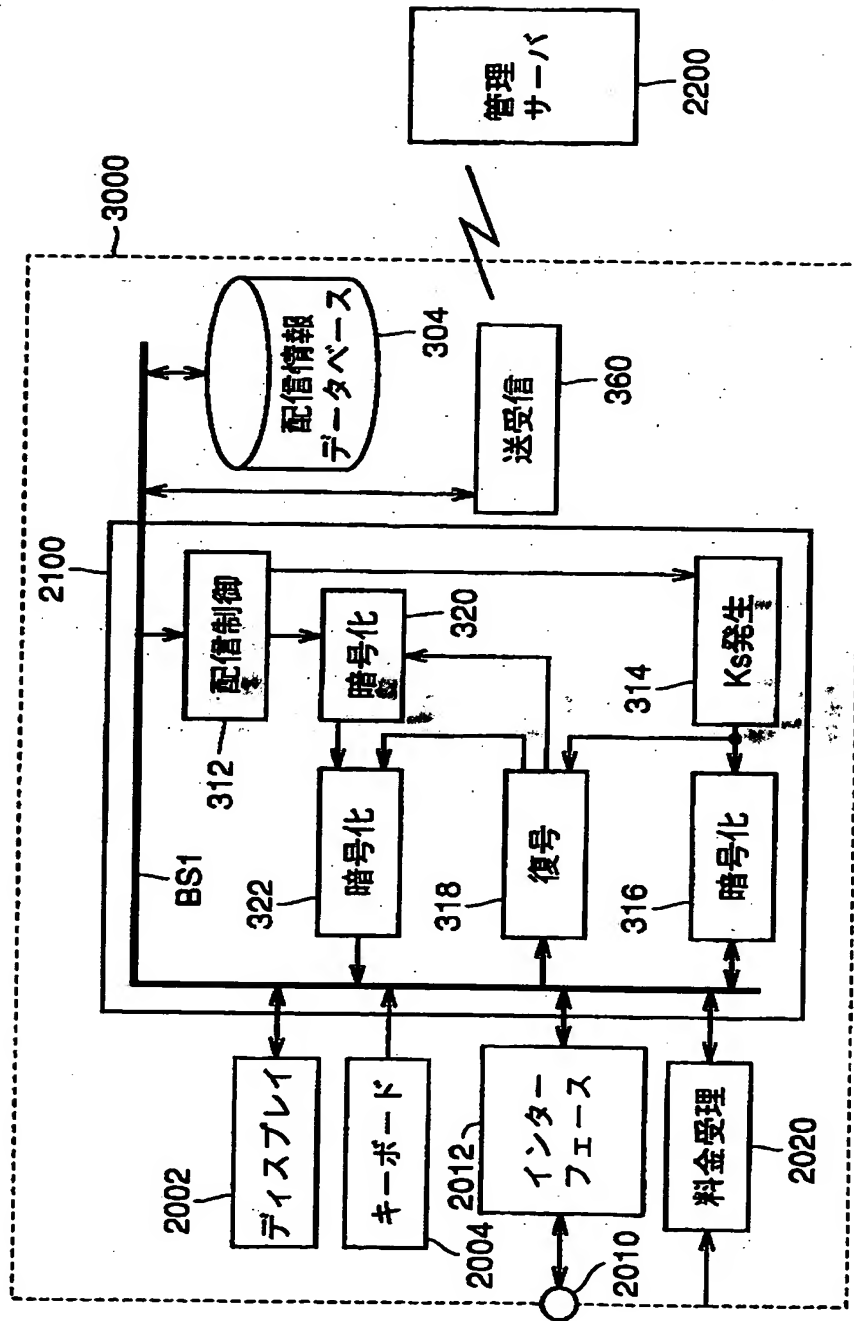
【図 2 5】



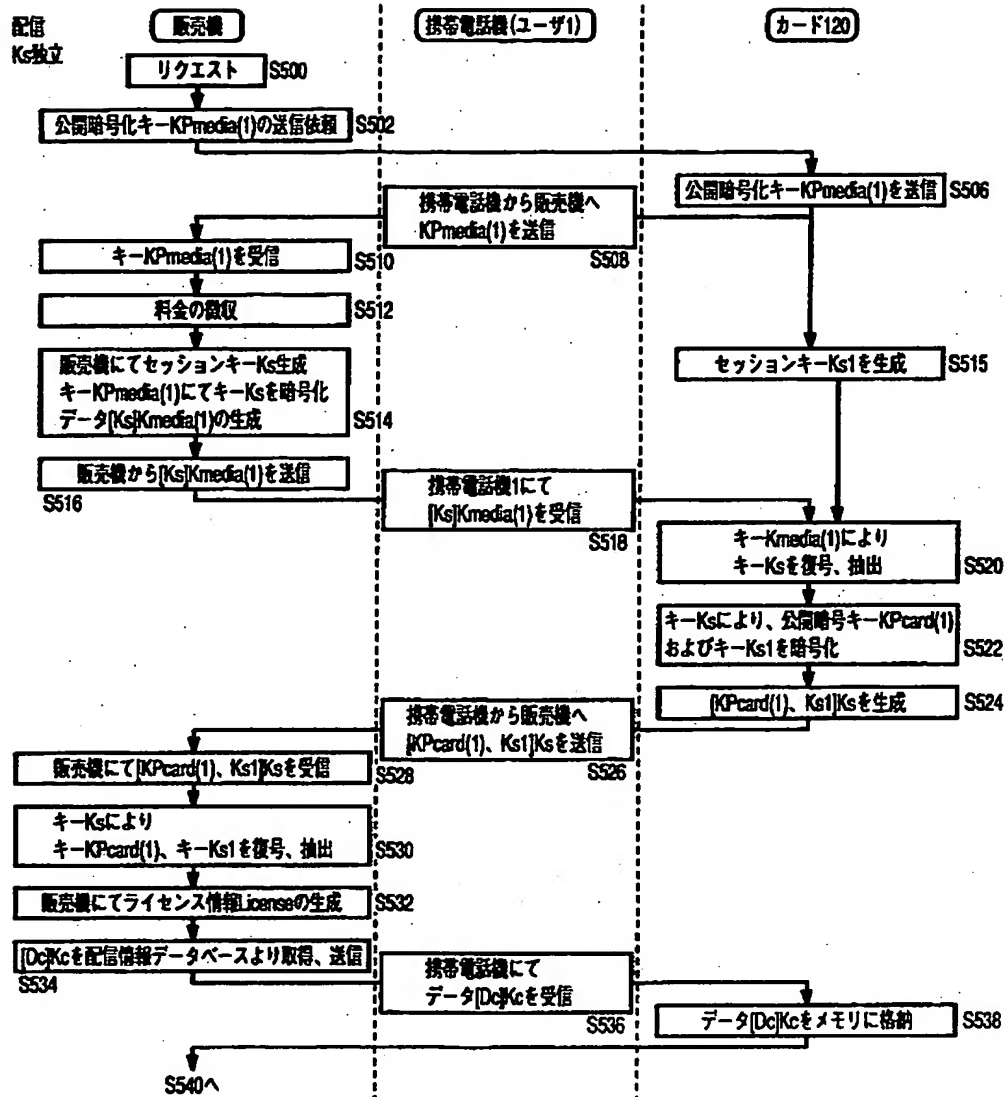
【図 2 6】



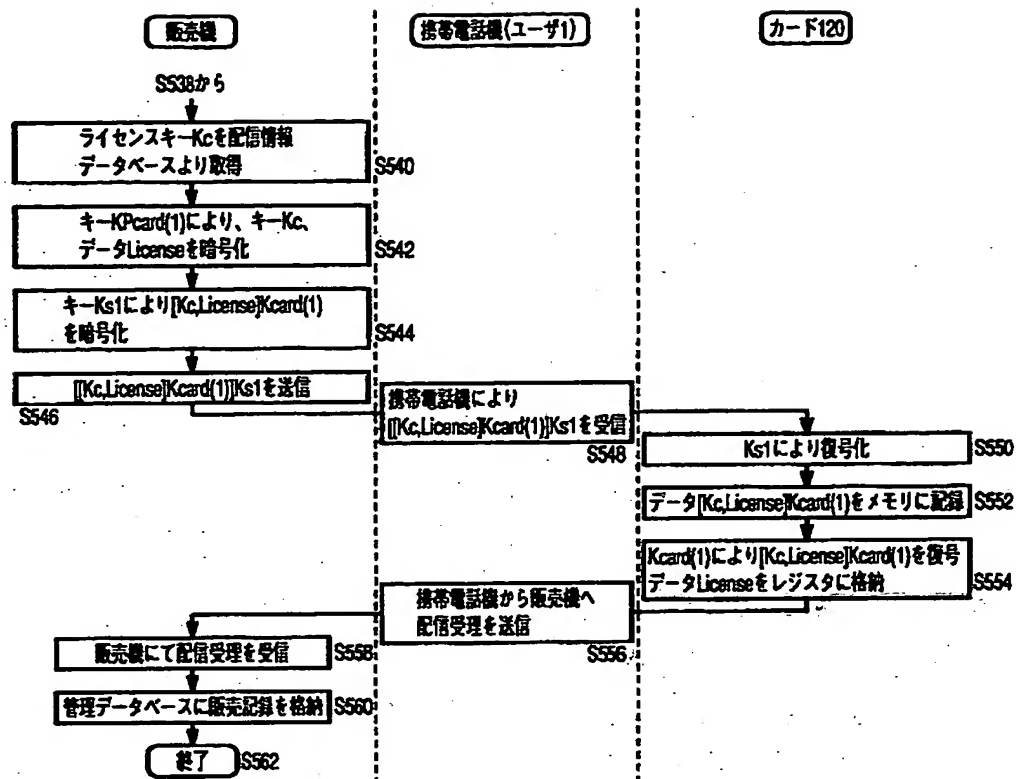
【図 27】



【図 2 8】

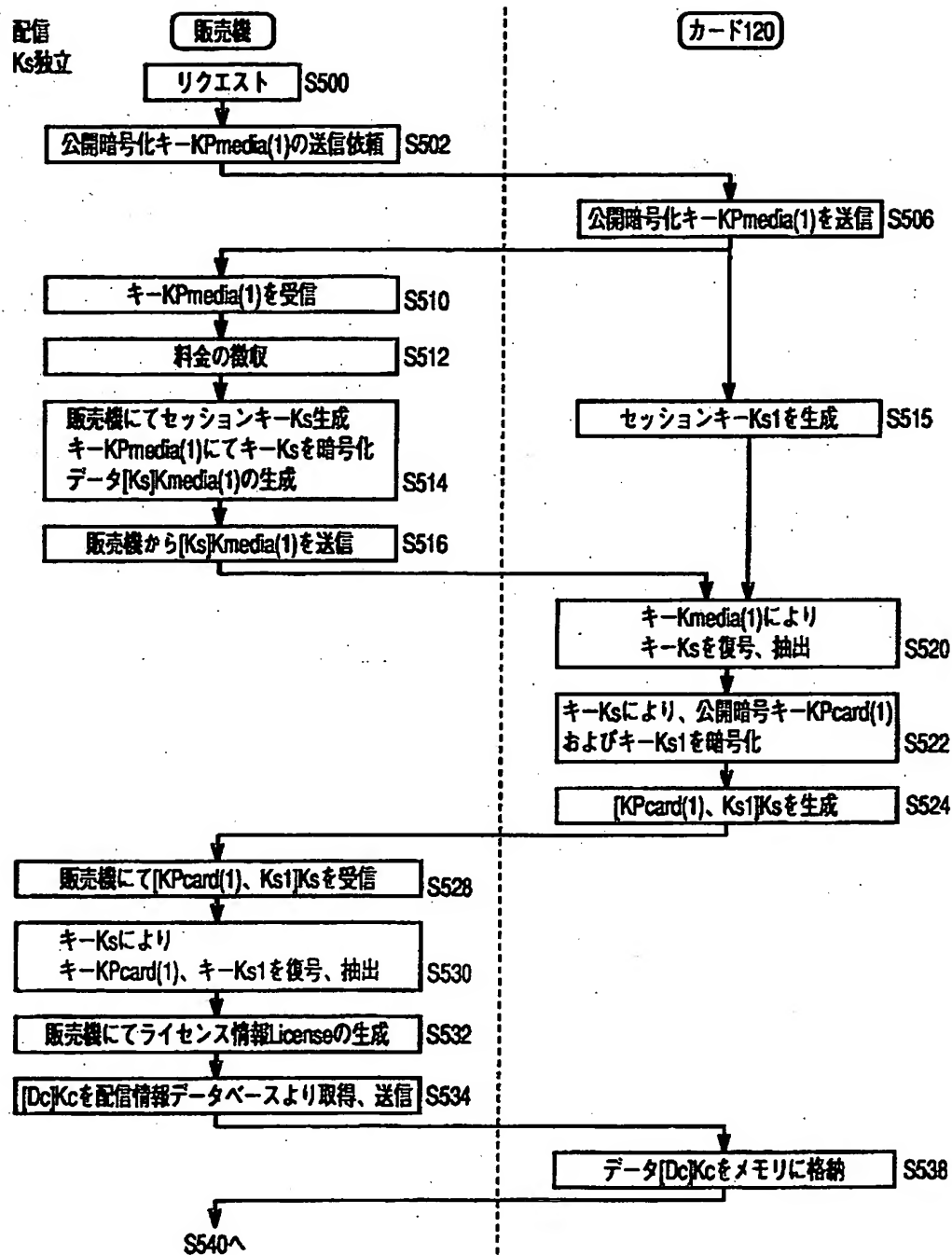


【図 2 9】

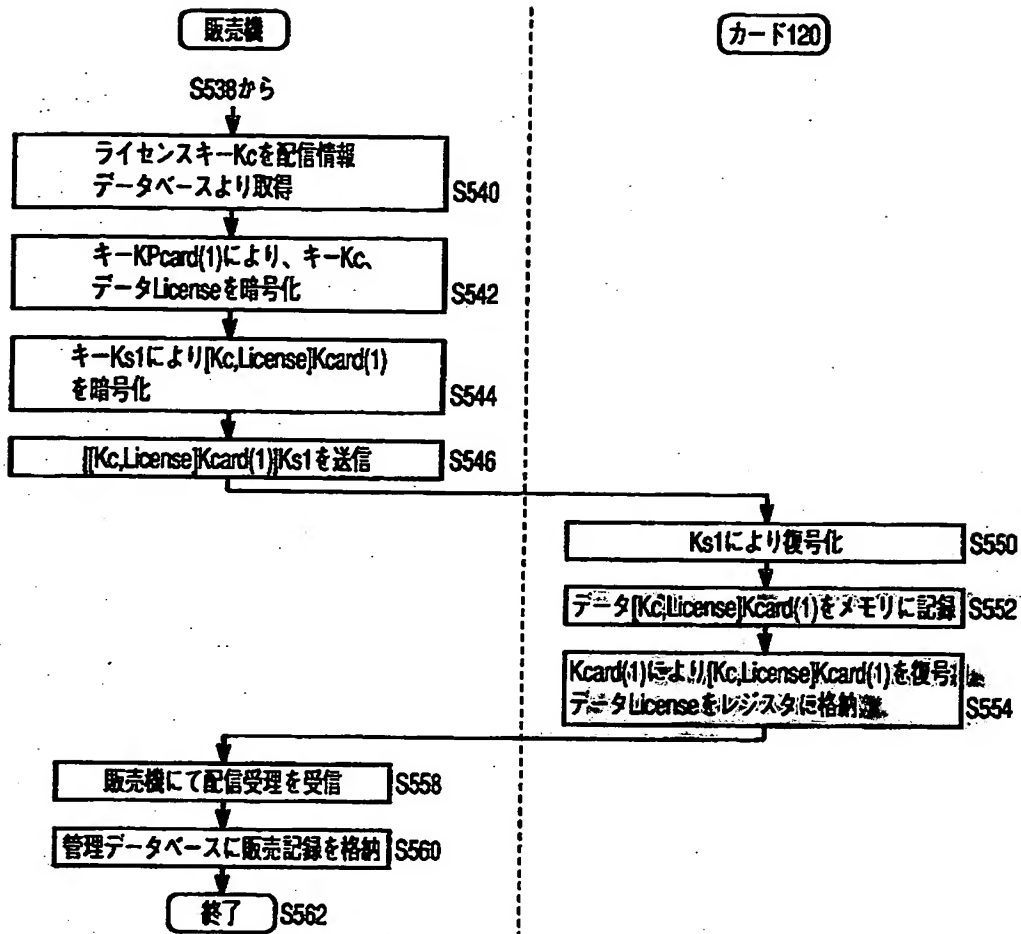




【図 3 0】

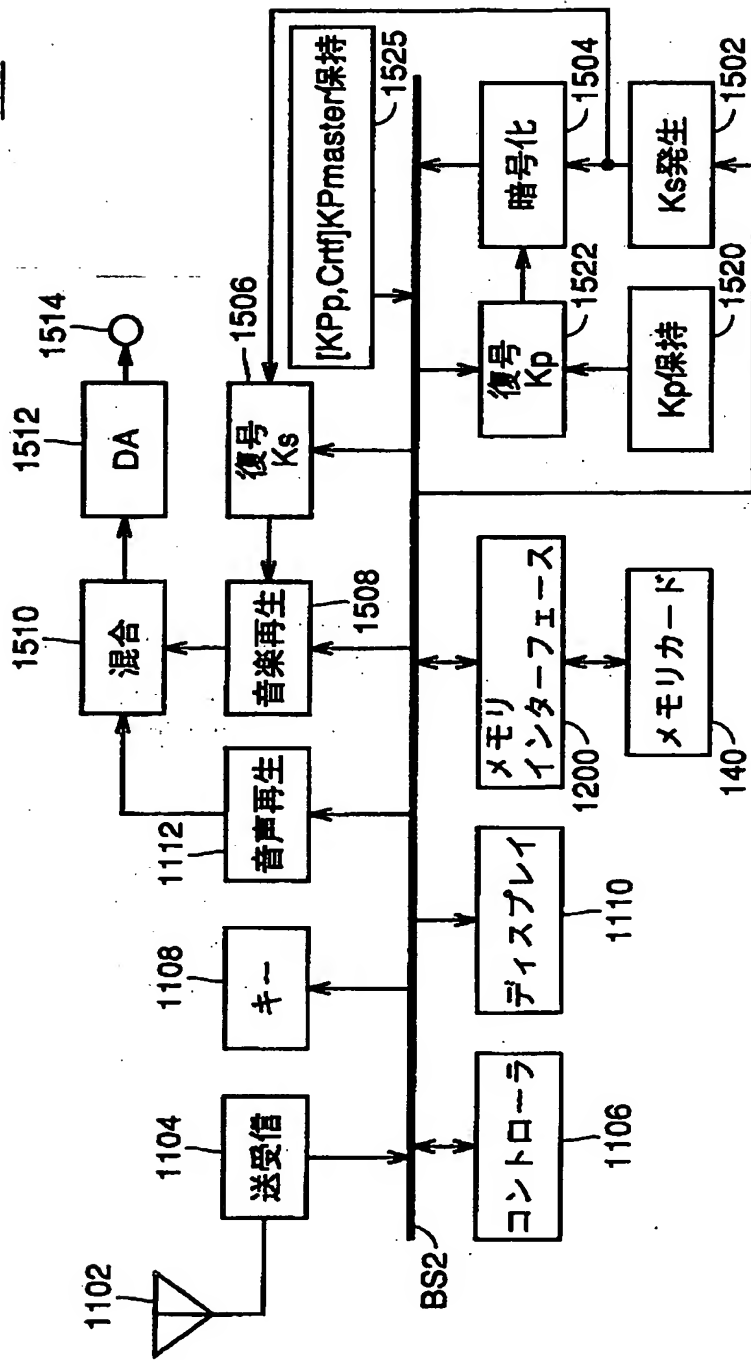


【図 3 1】



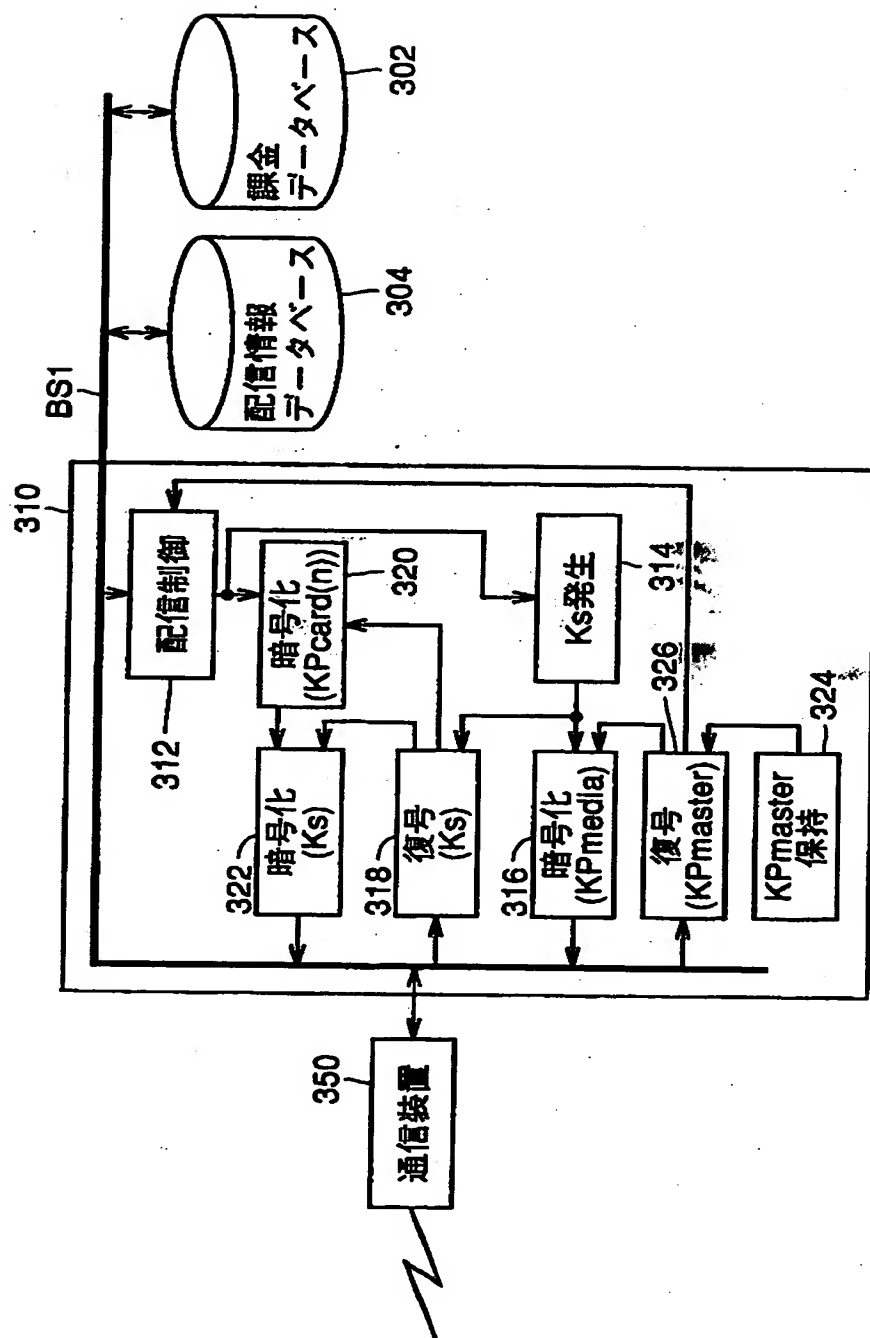
【図 3 2】

105

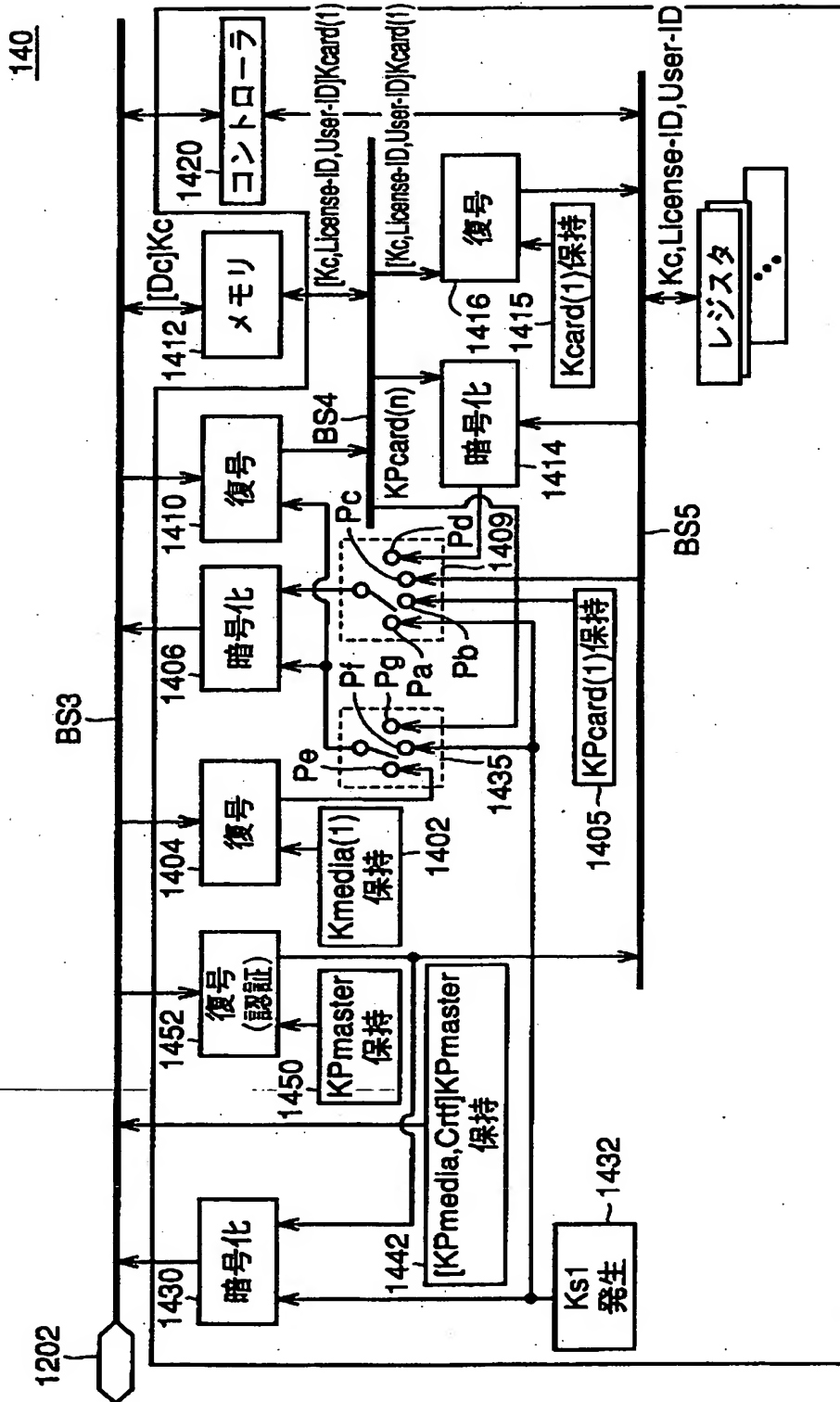


【图 3 3】

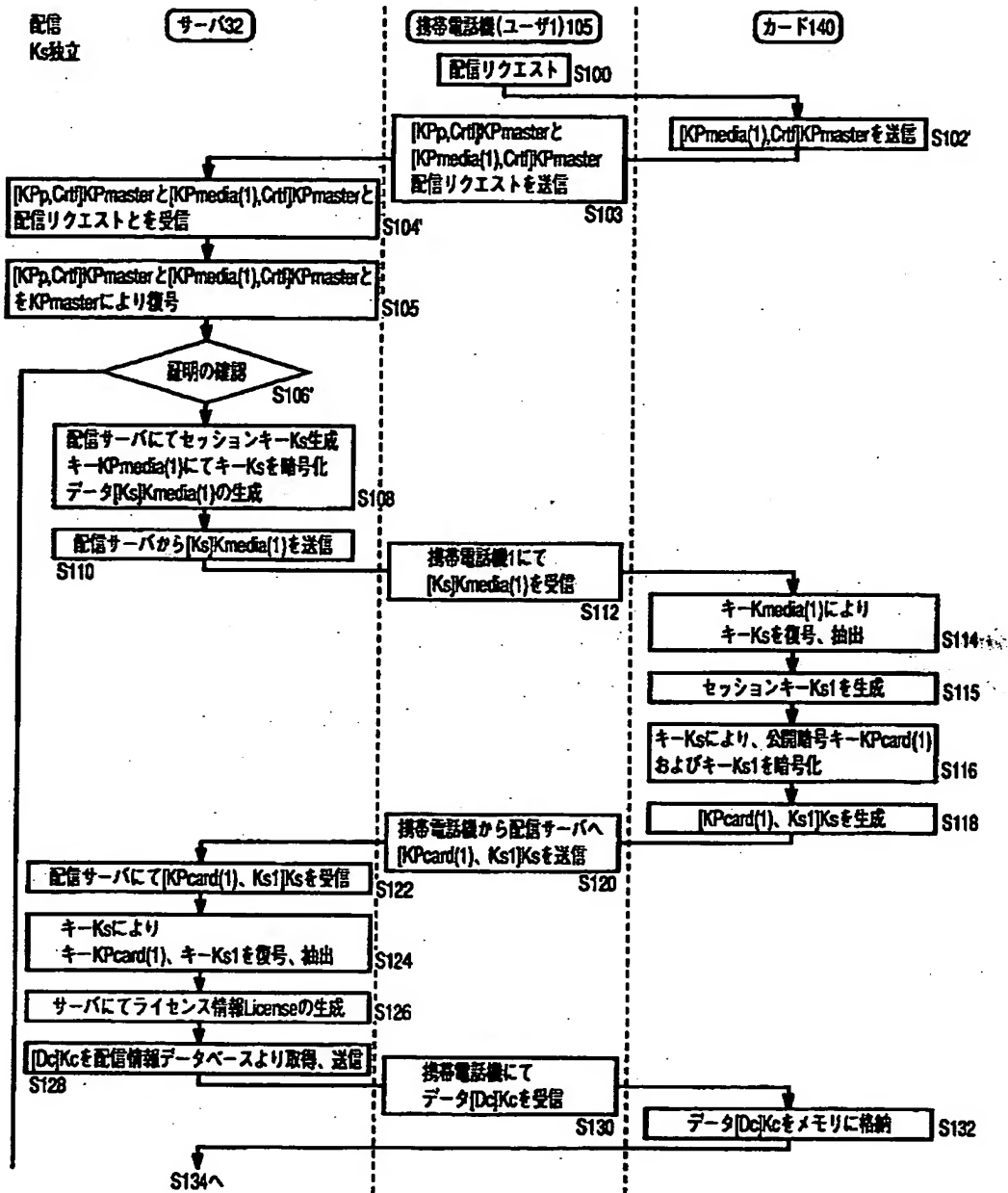
12



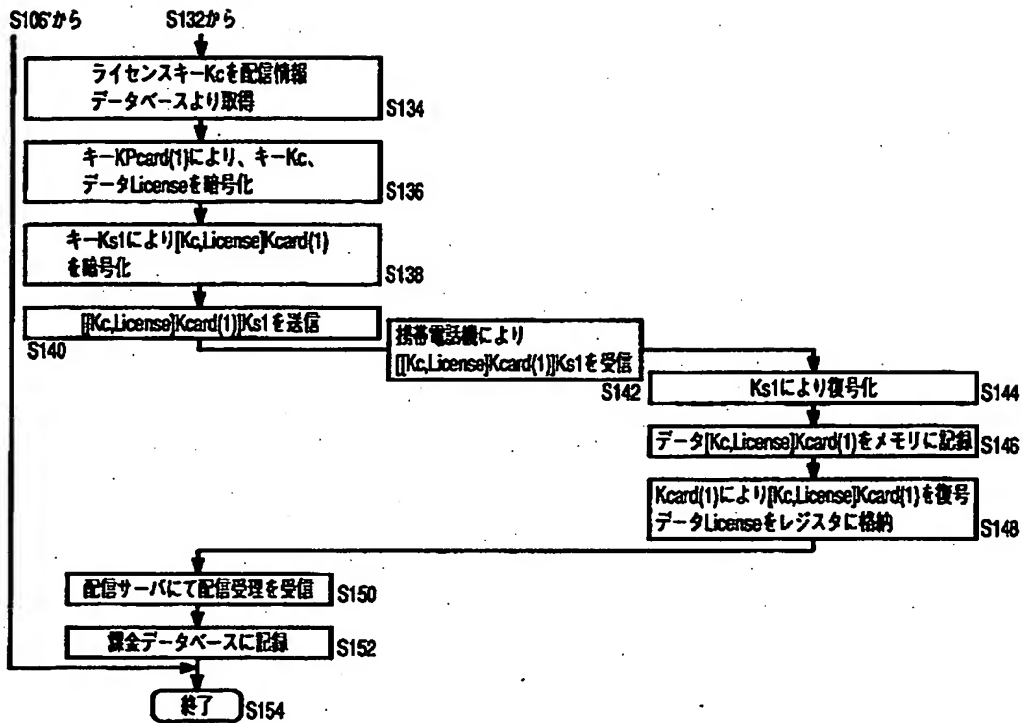
【図 3 4】



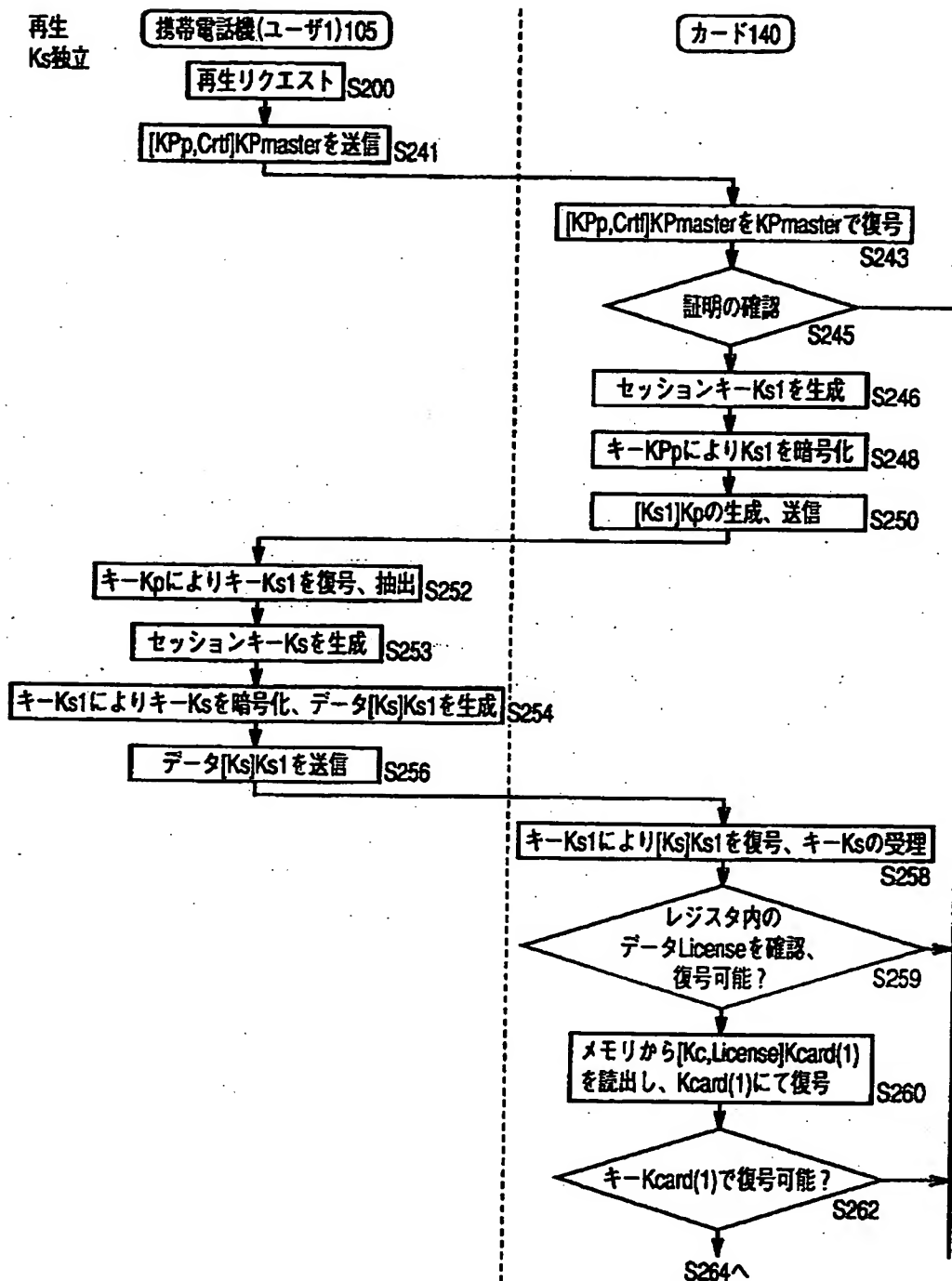
【図 3 5】



【図 3 6】

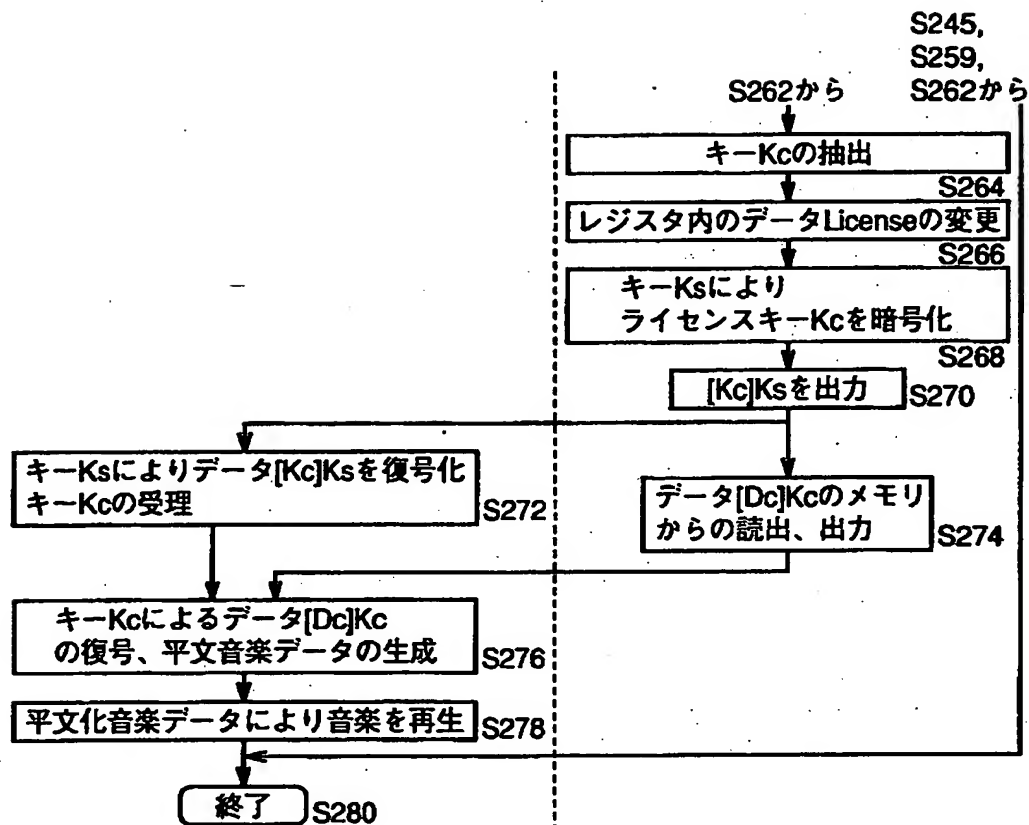


【図 3 7】

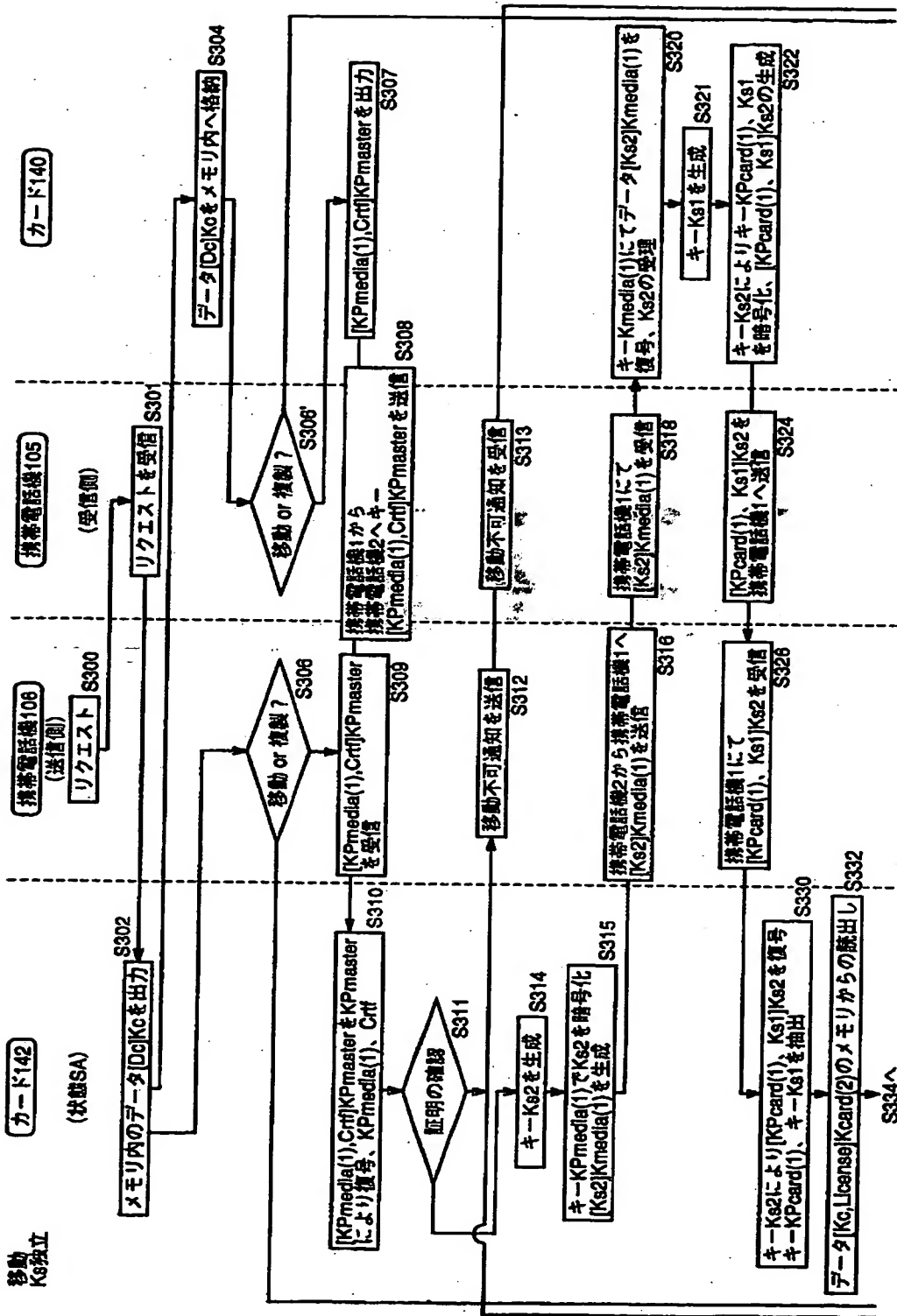




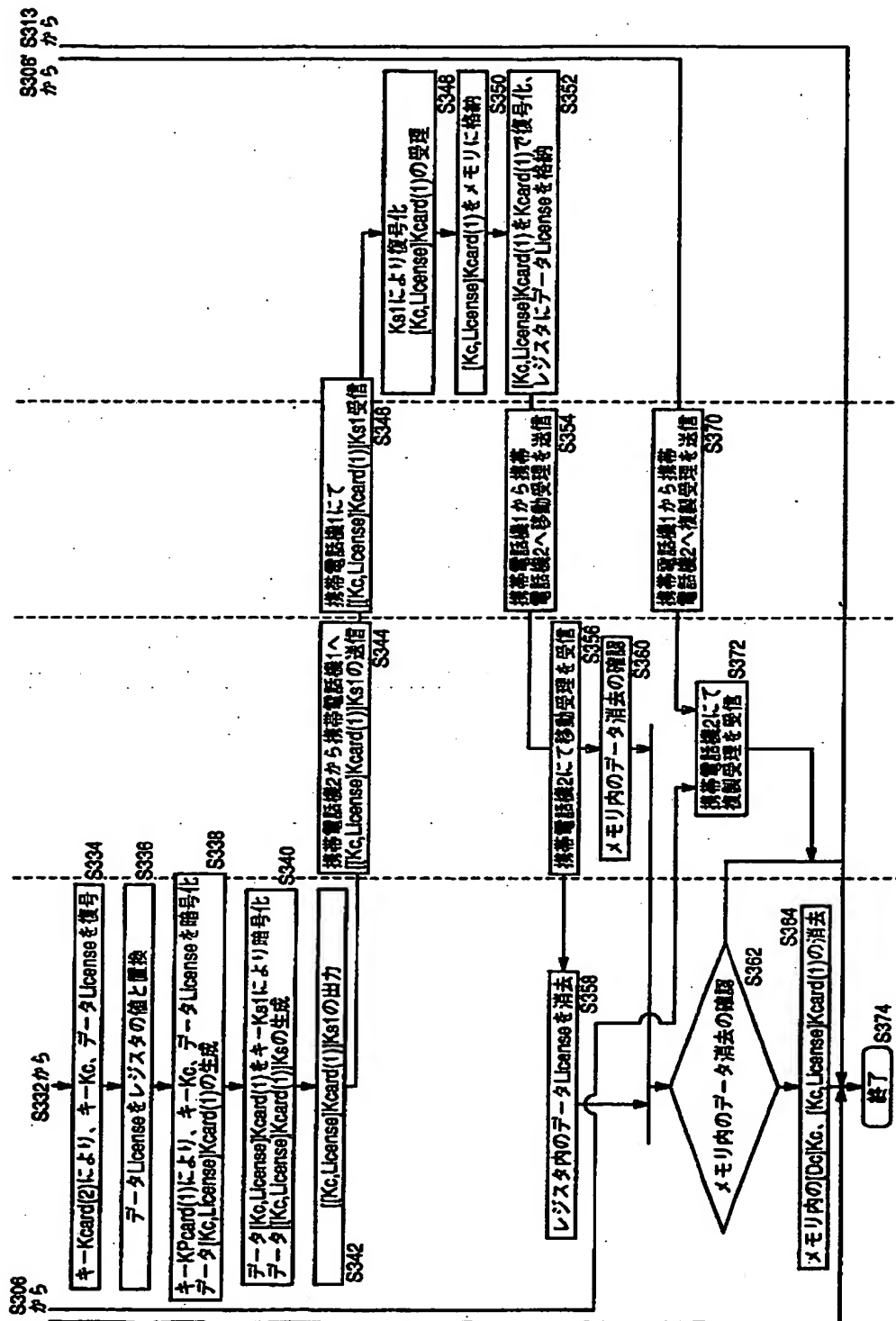
【図 3 8】



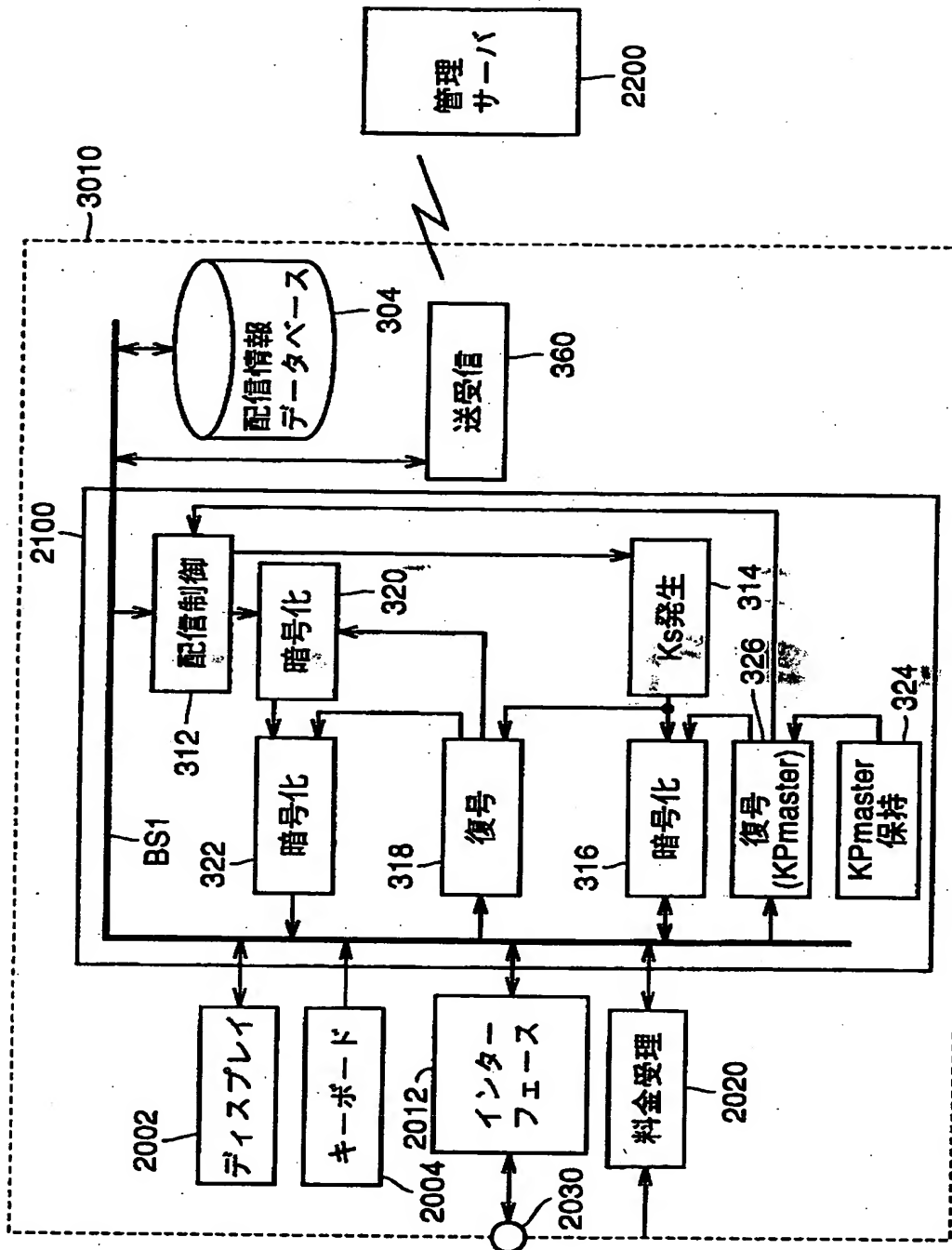
【図 3 9】



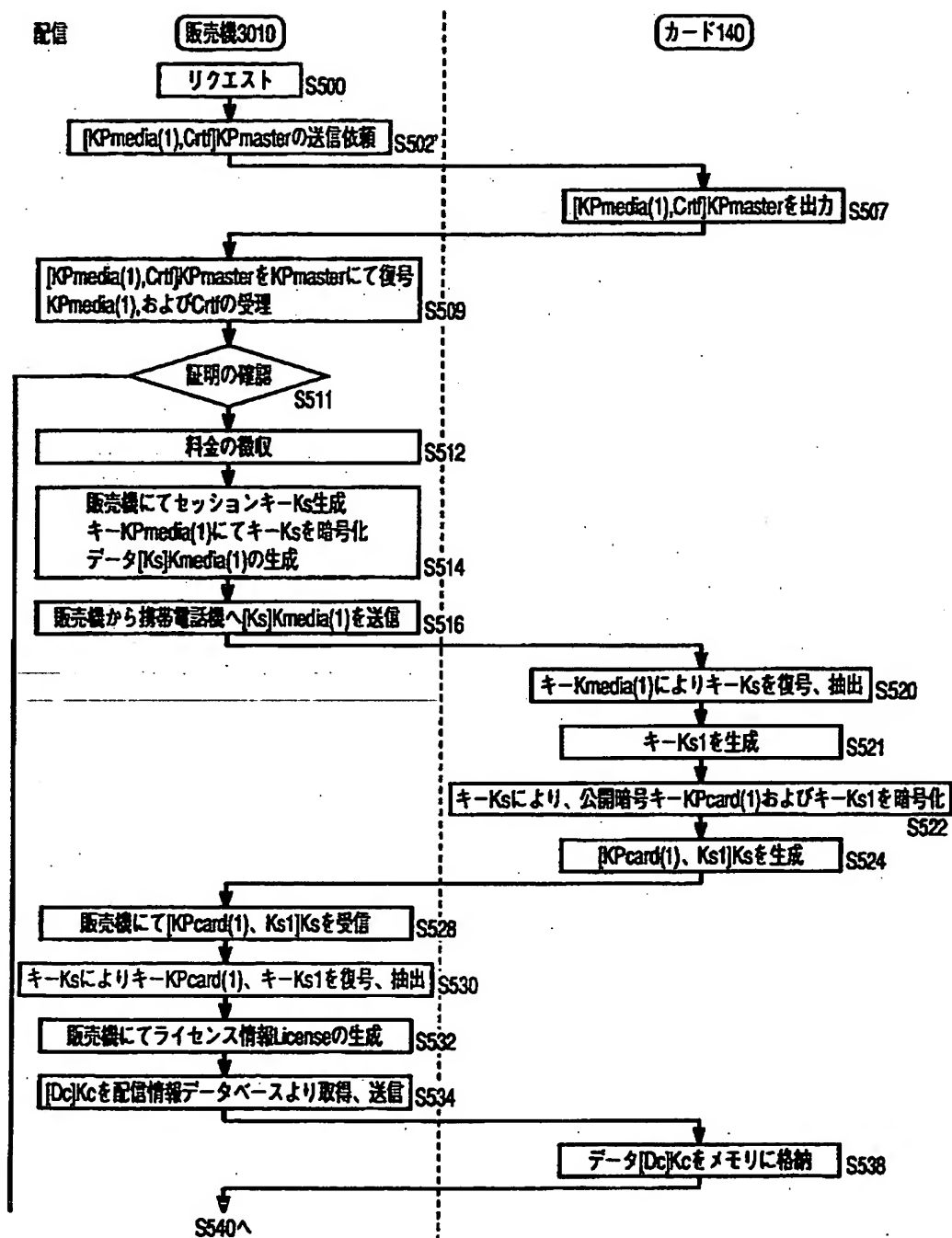
【図 4 0】



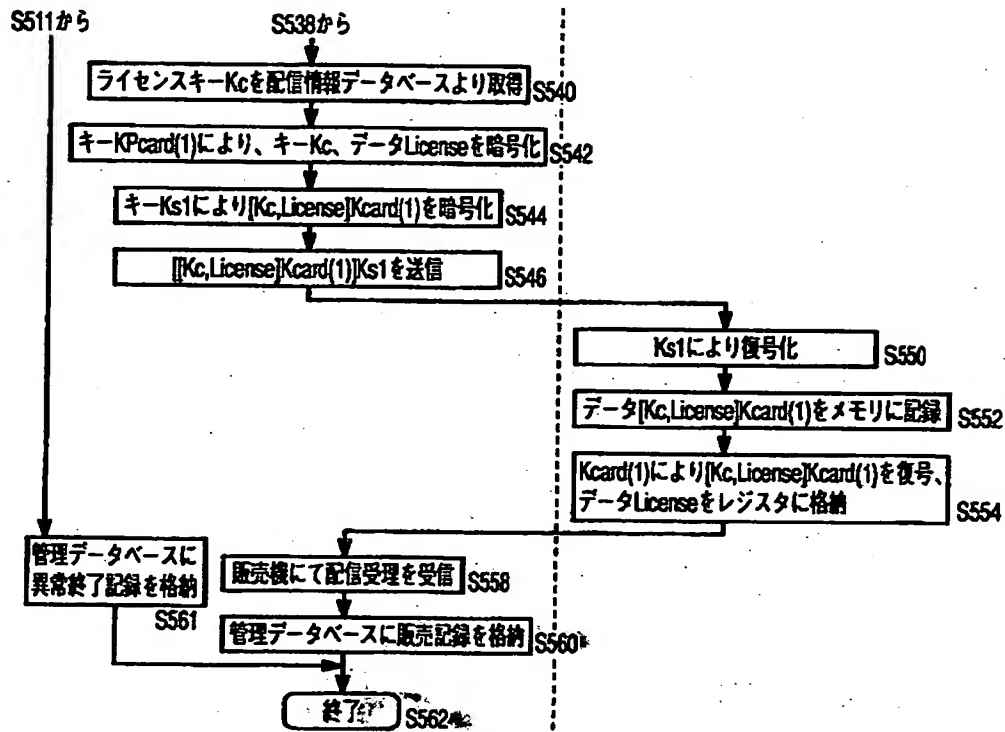
【図 4 1】



【図 4 2】

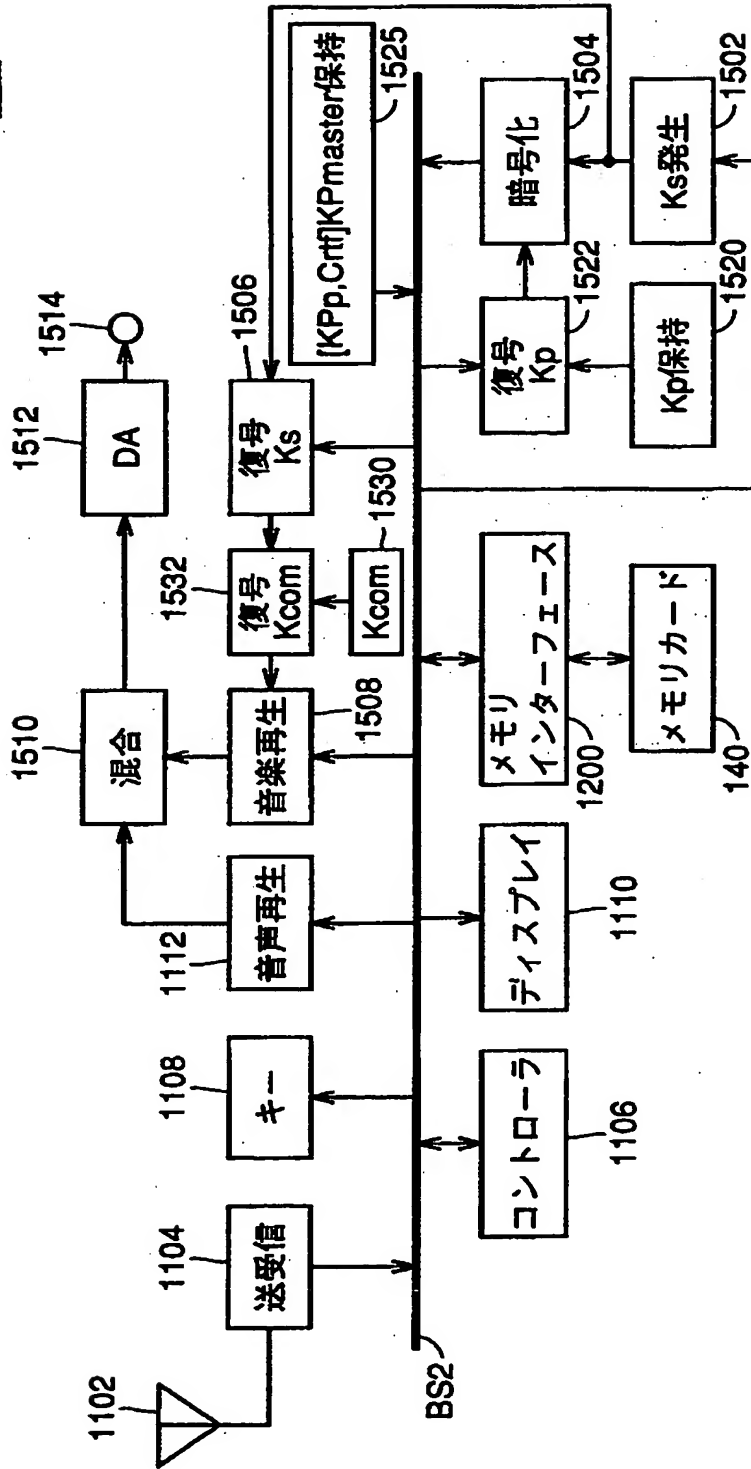


【図 4 3】



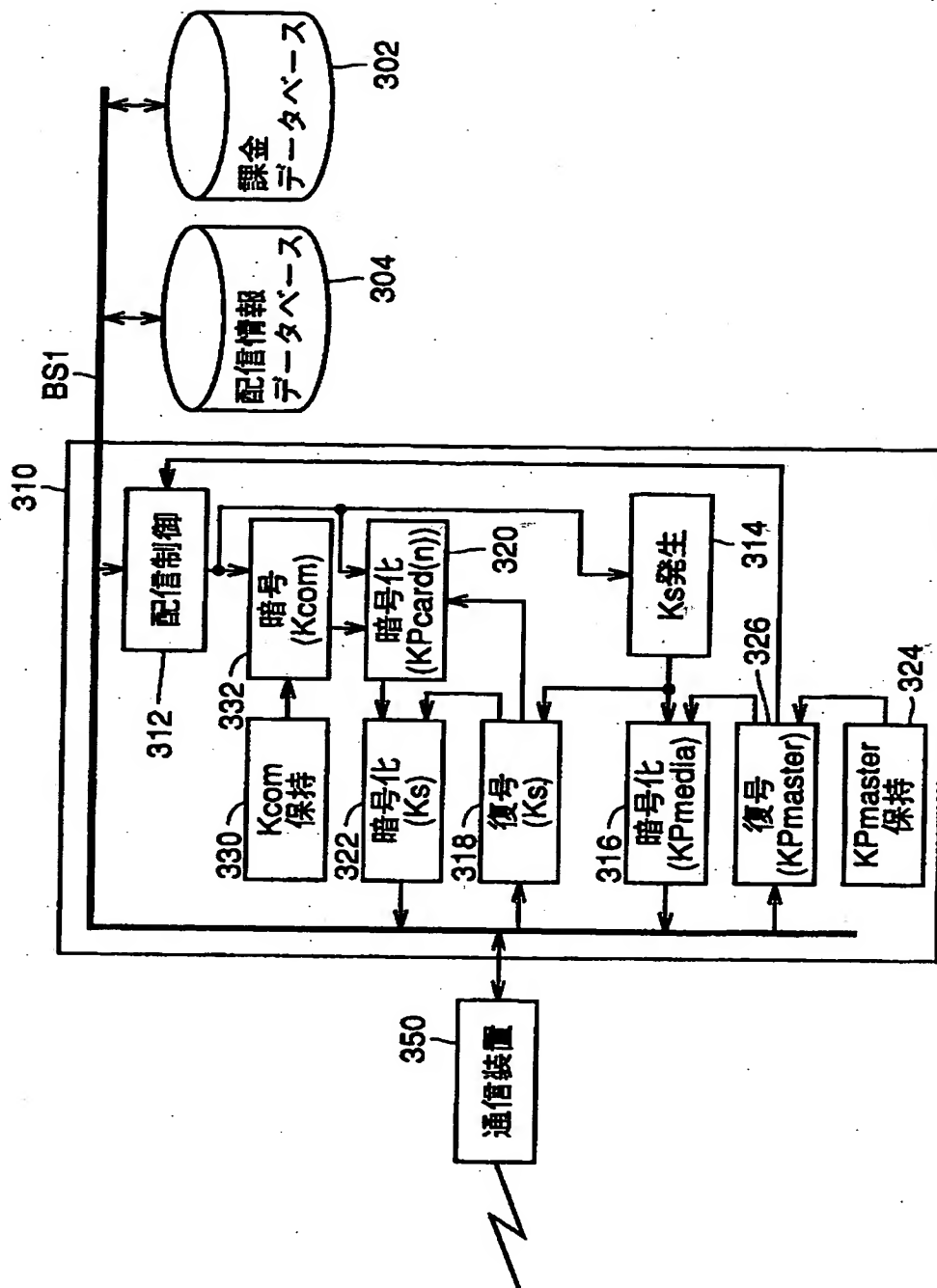
【図 4 4】

107



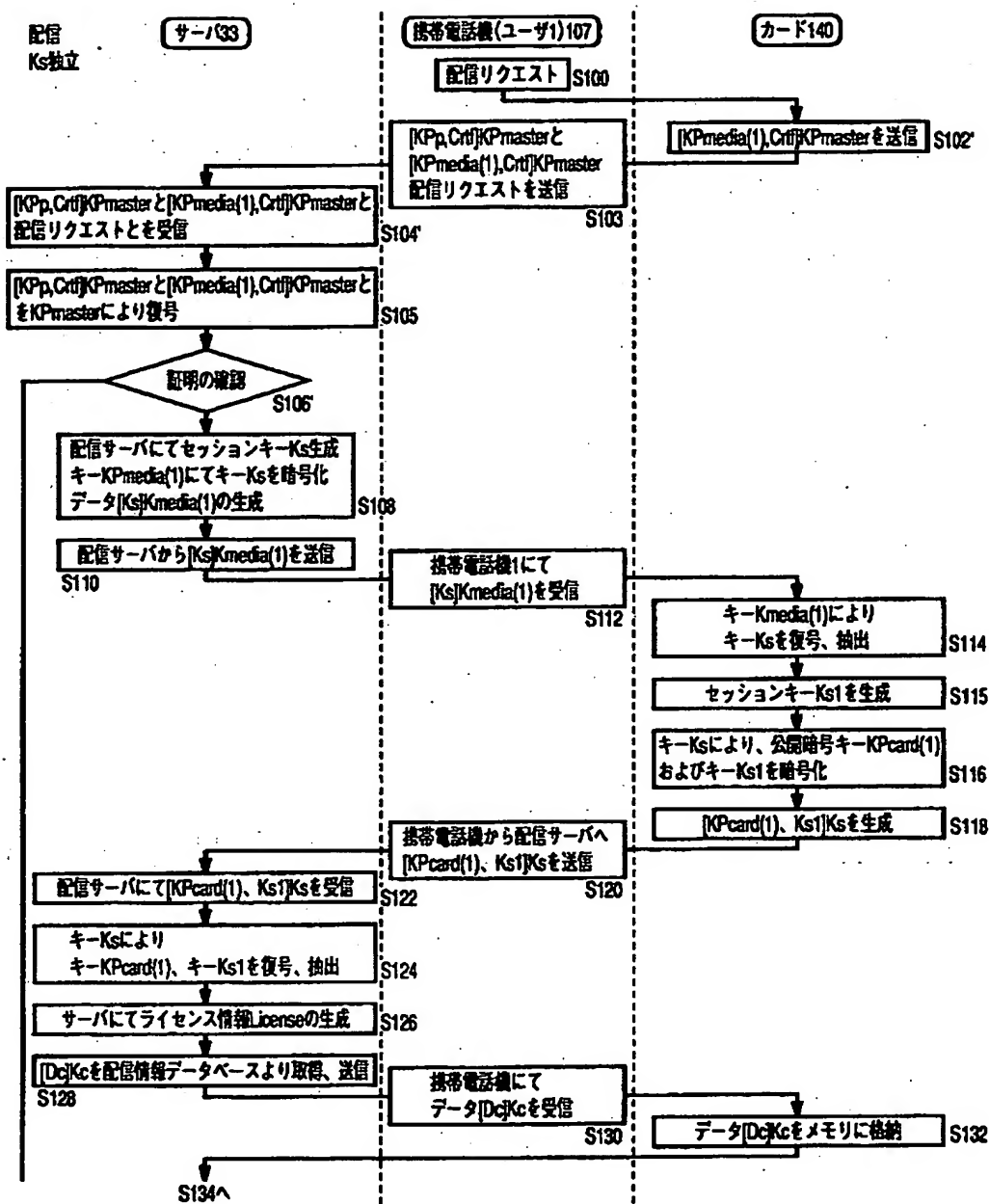
【図 4 5】

13

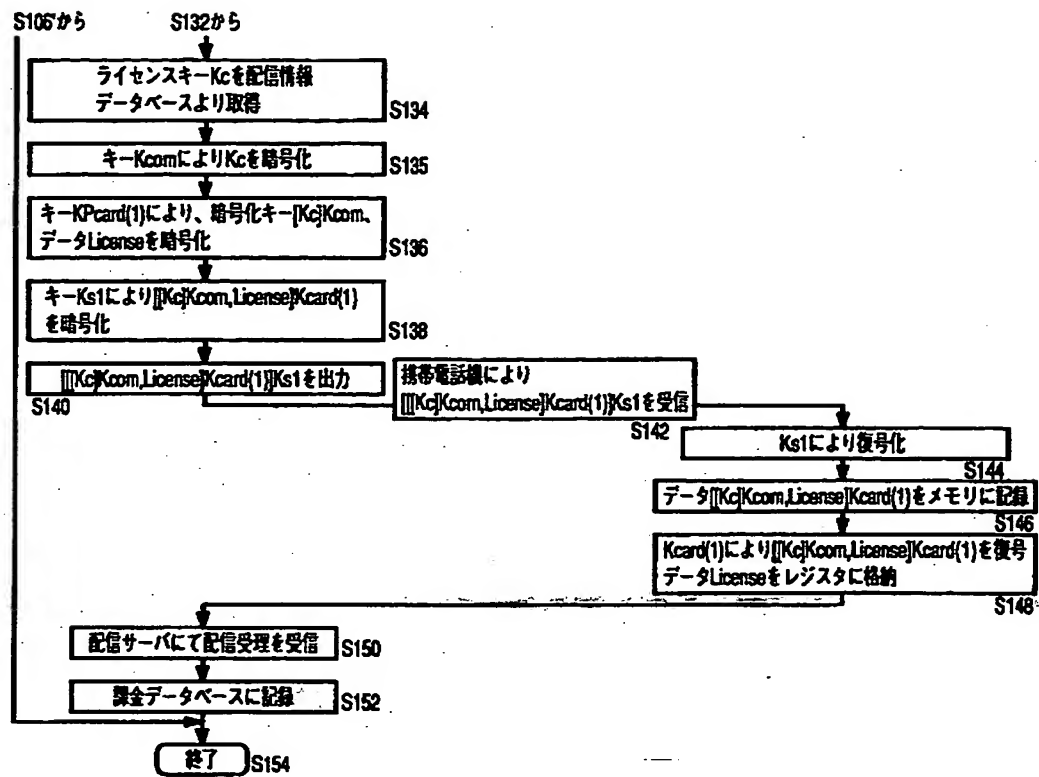




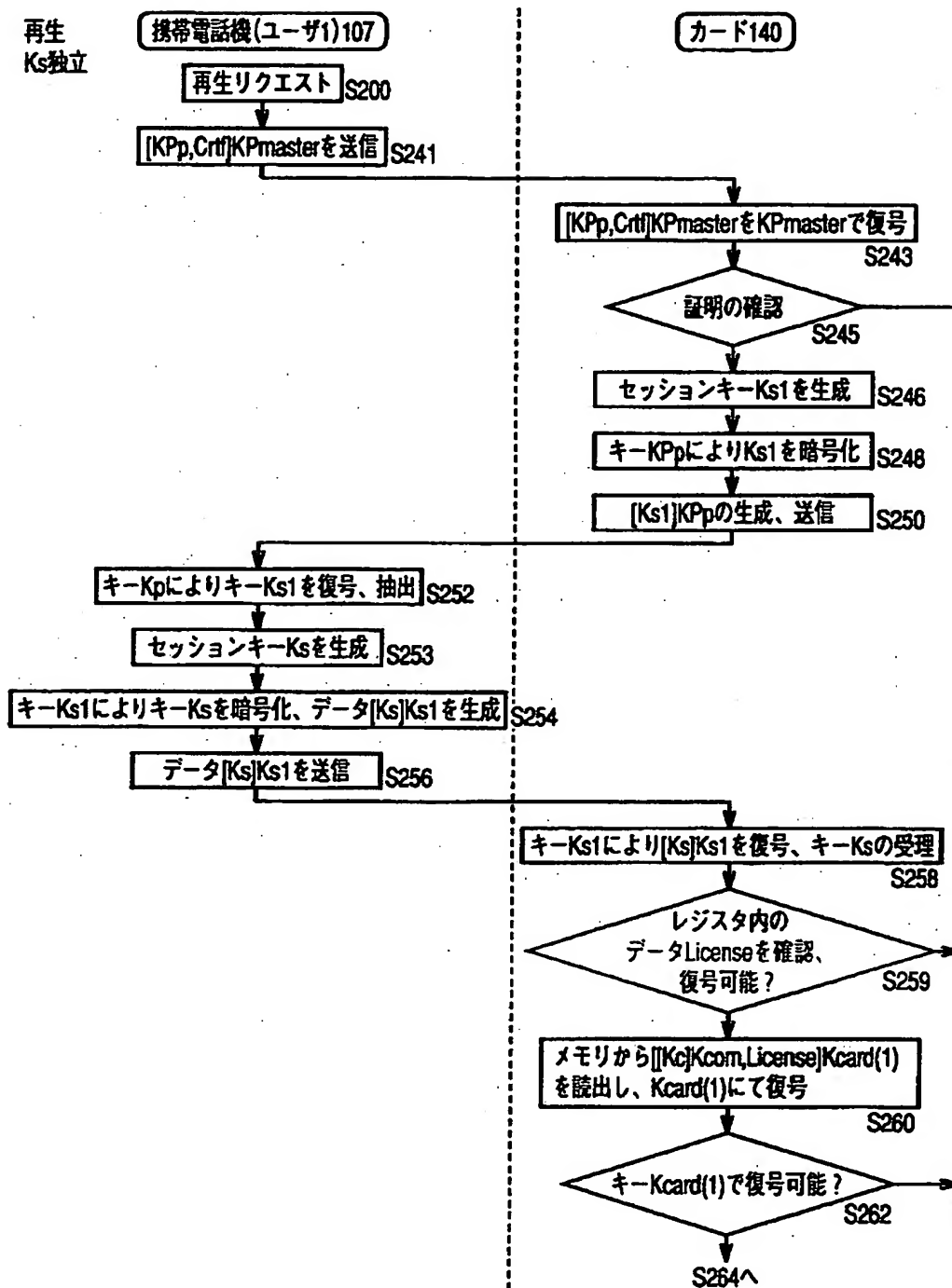
【図 4 6】



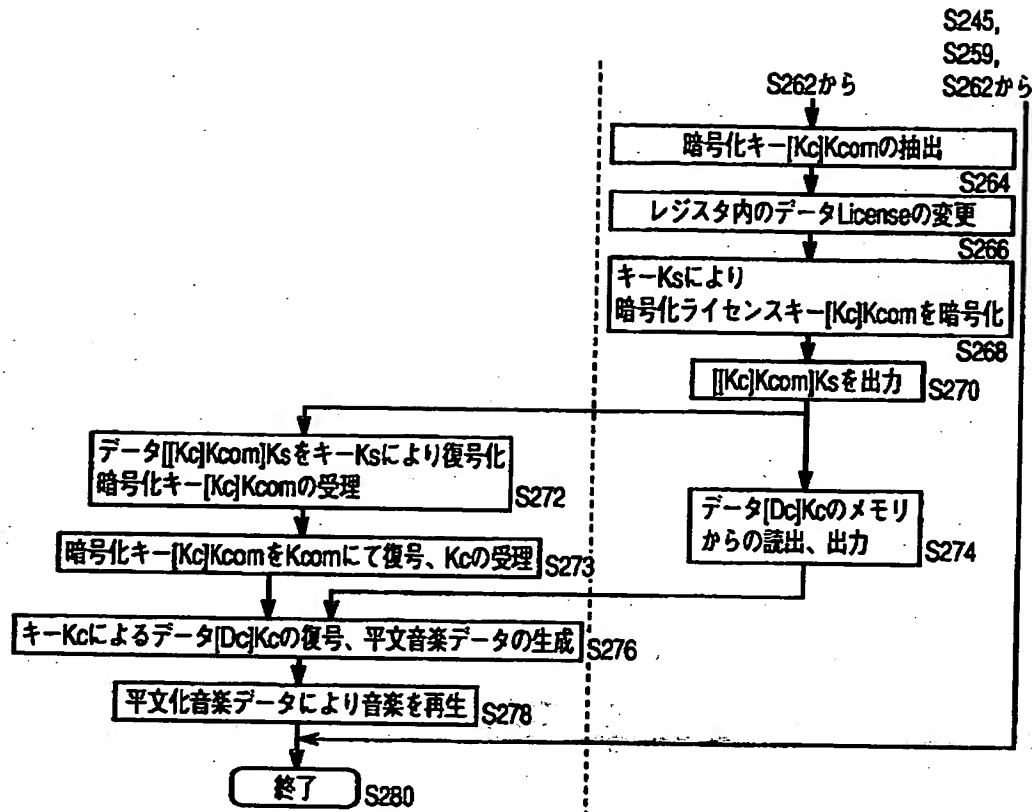
【図 4 7】



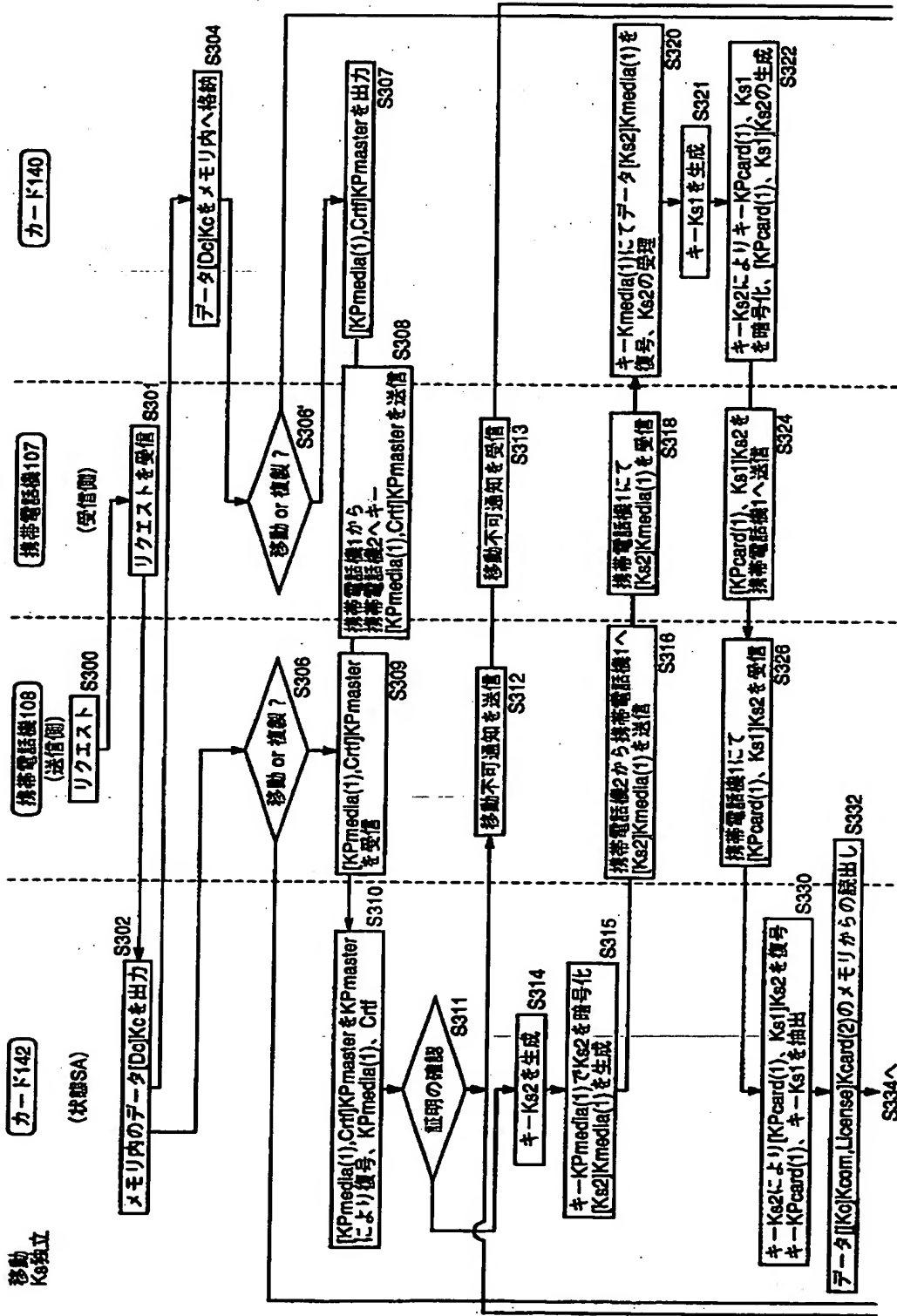
【図 4 8】



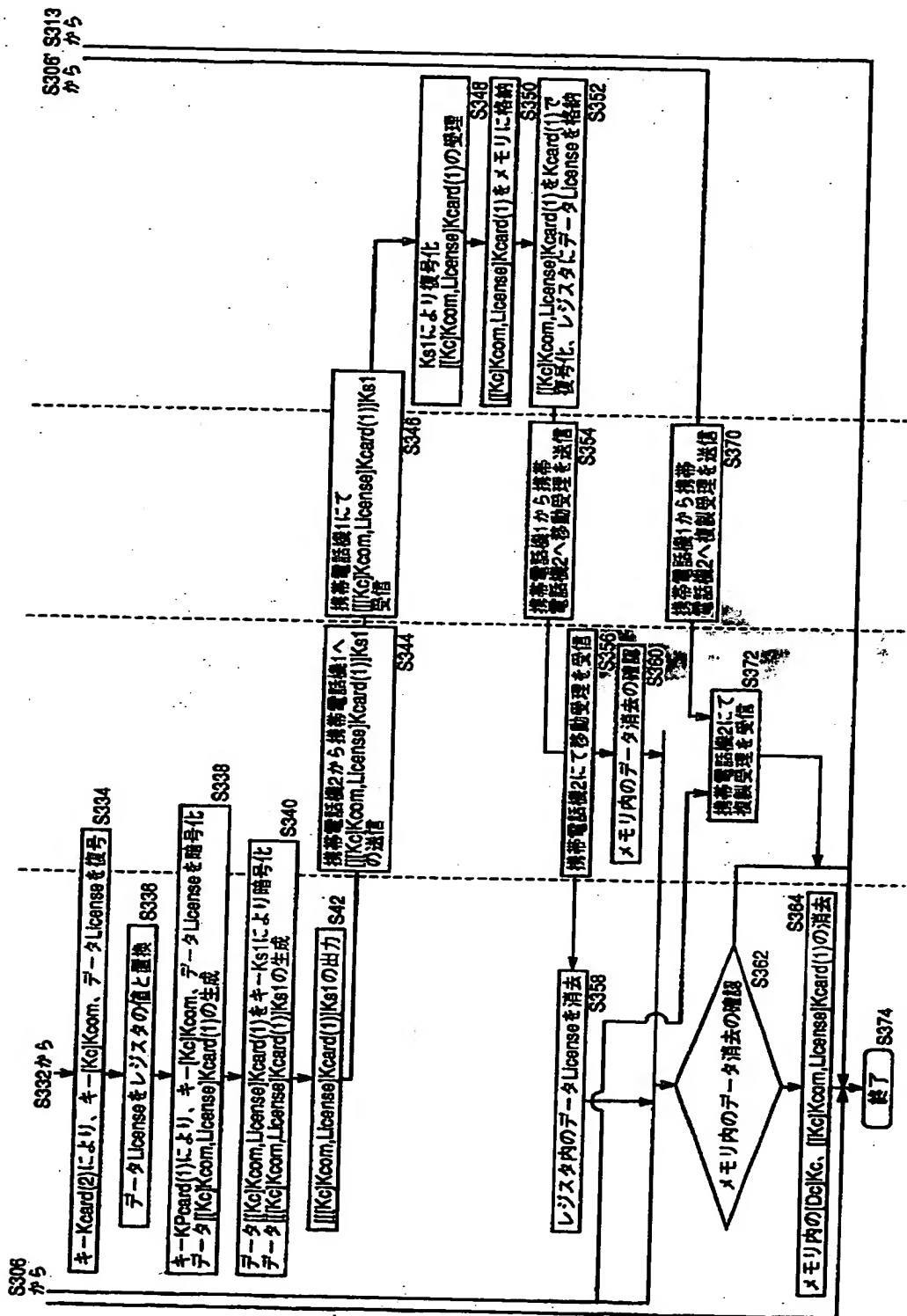
【図 4 9】



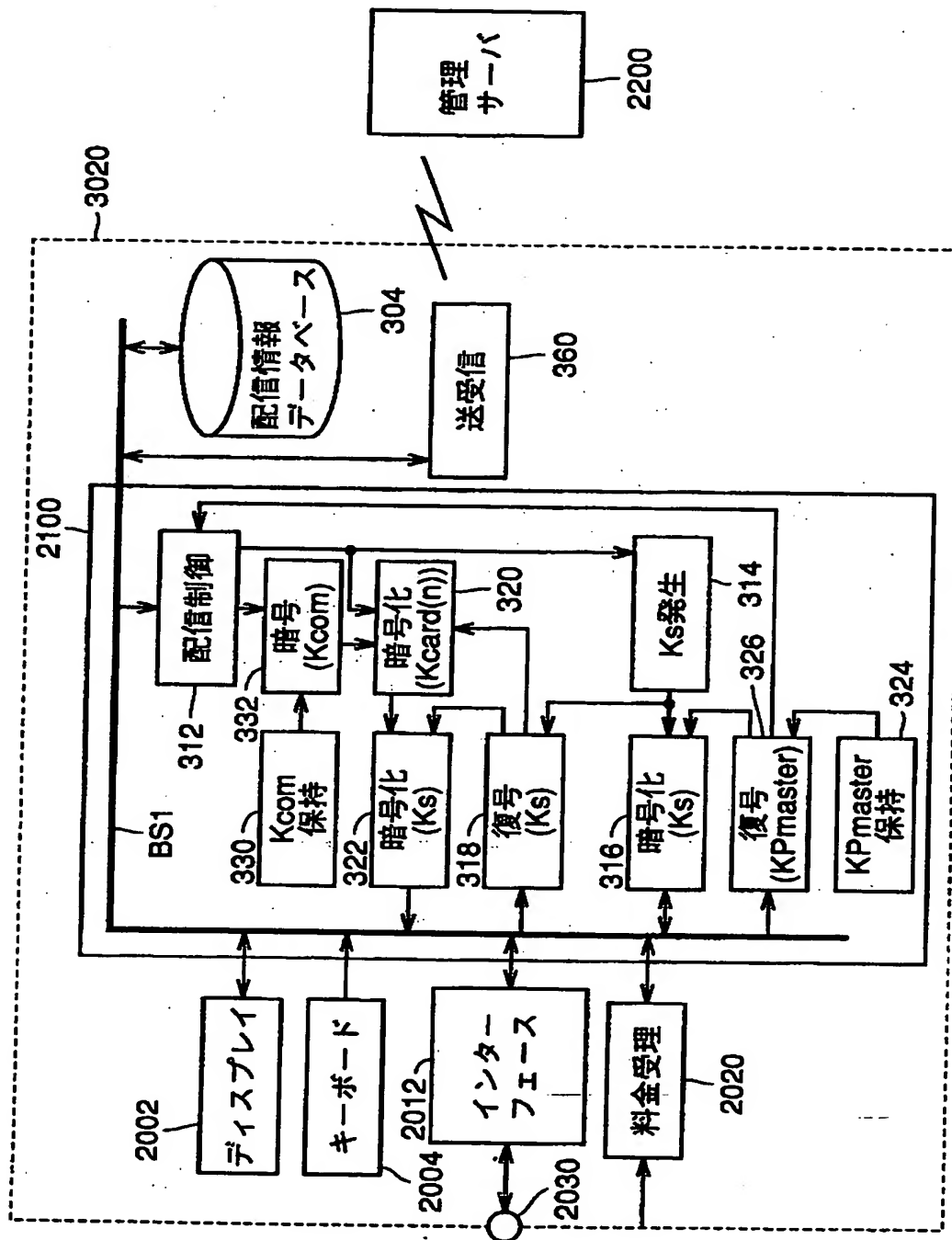
【図 50】



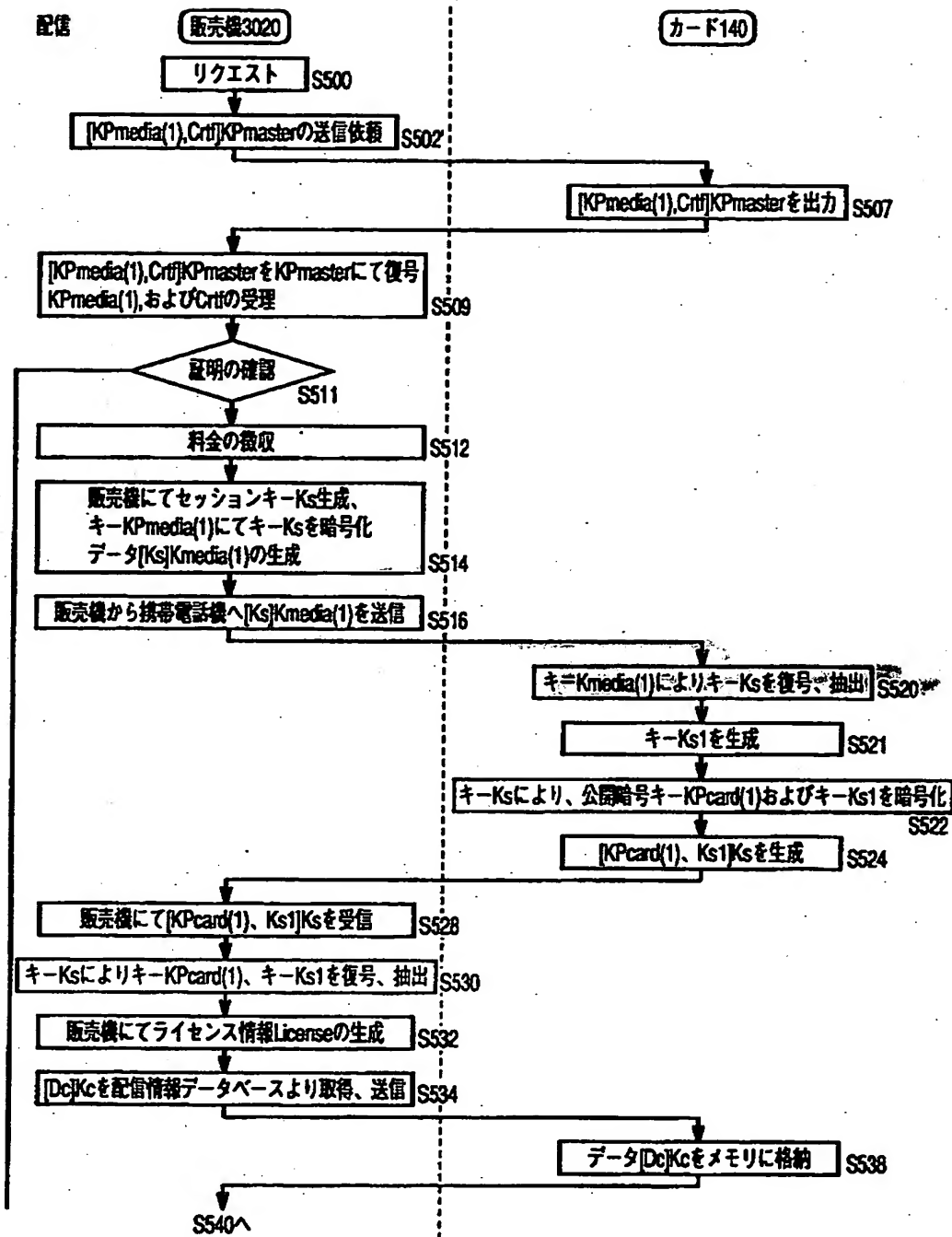
【図 51】



【図 5 2】

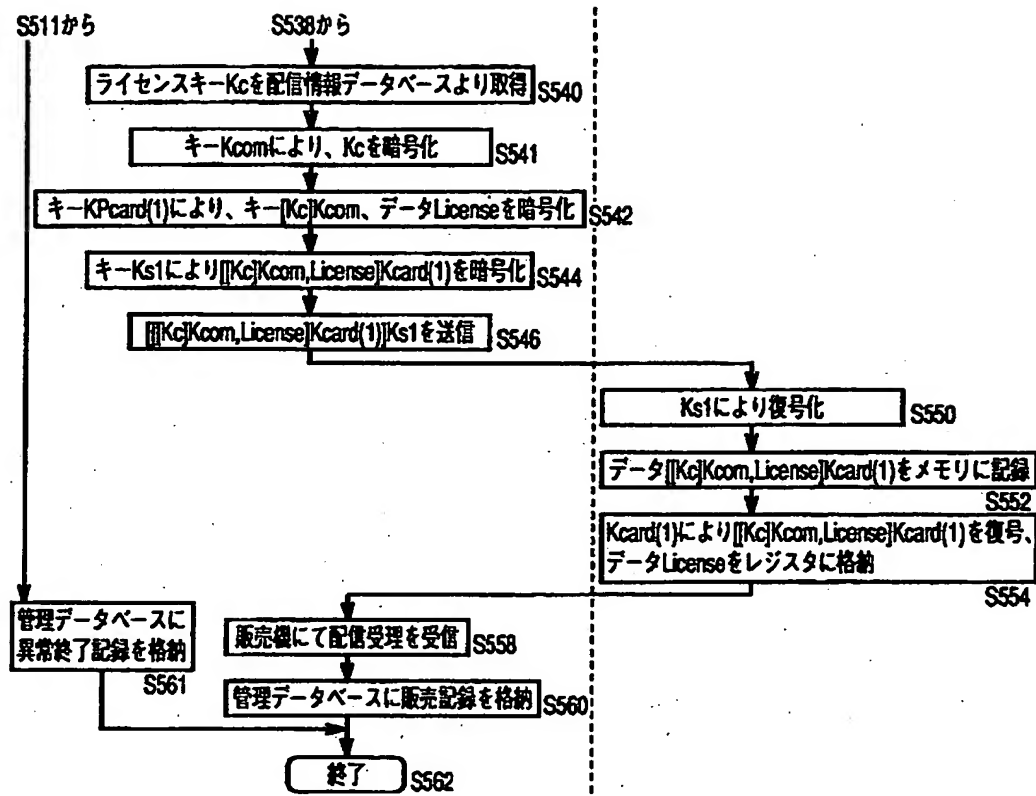


【図 5 3】

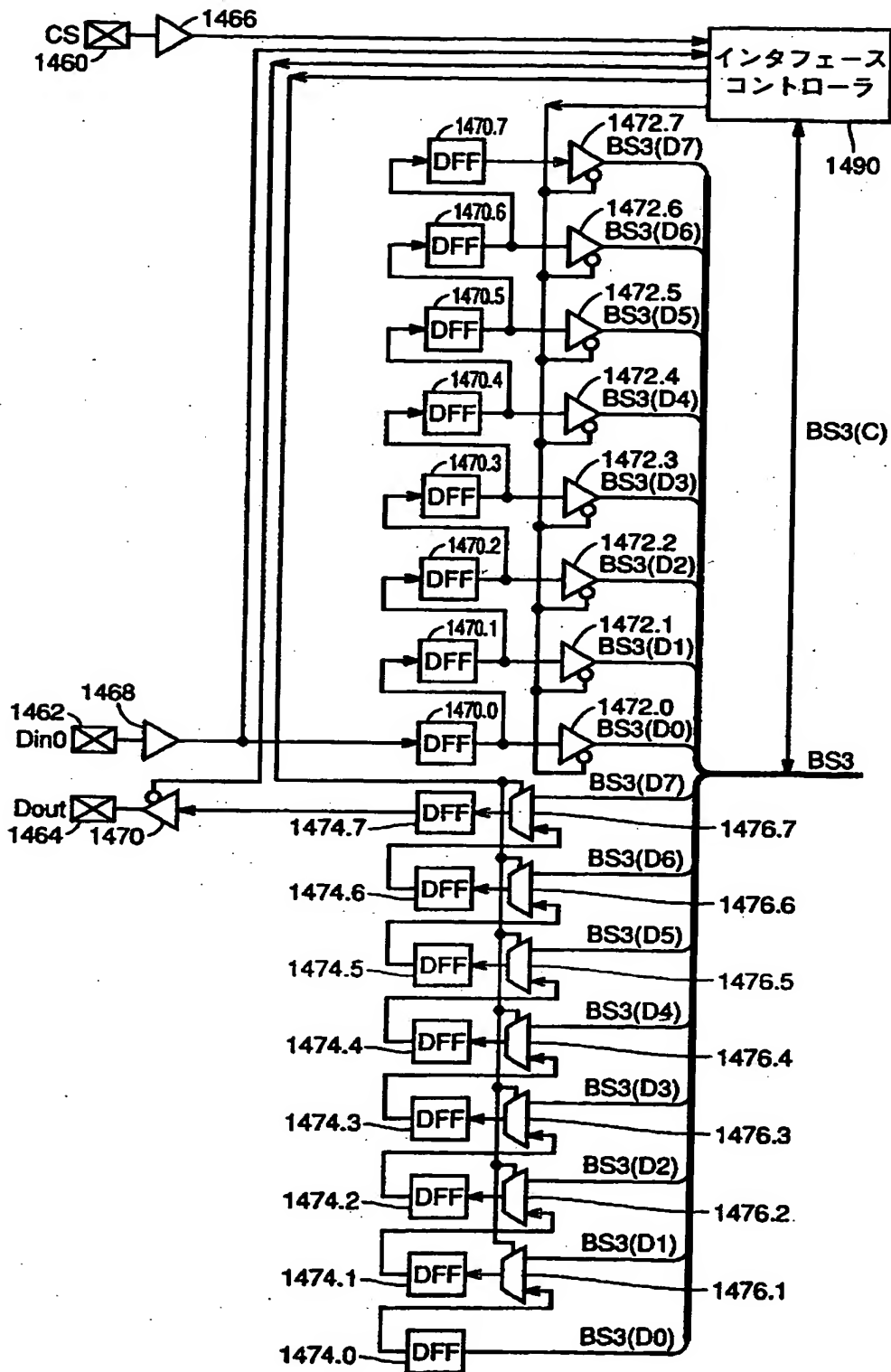




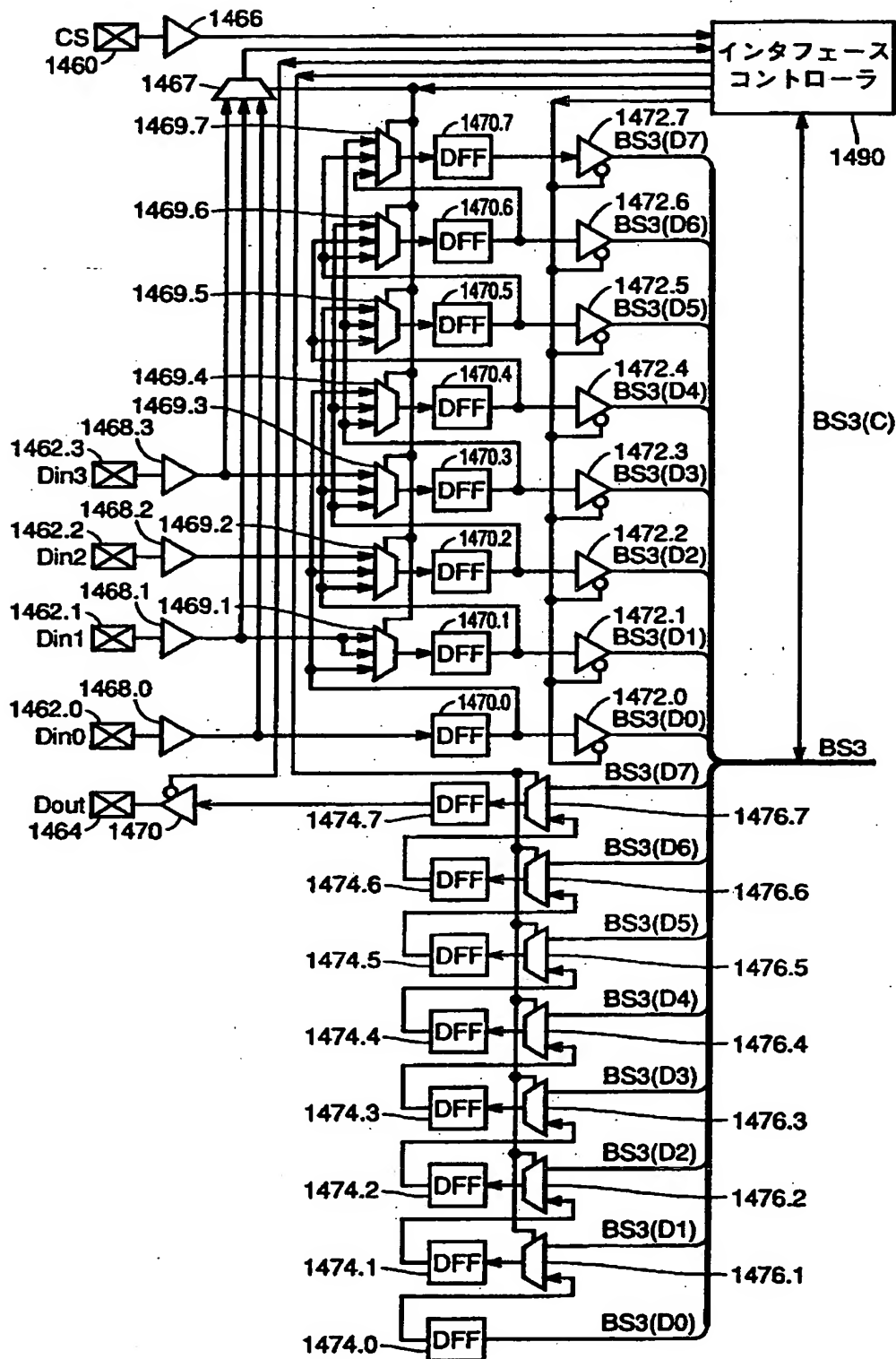
【図 5 4】



【図 5 5】



【図 5 6】



【書類名】 要約書

【要約】

【課題】 著作権者の許可なく複製されることを防止することが可能な情報配信システムを提供する。

【解決手段】 メモリカード110は、サーバから携帯電話網を介してデータベースBS3に与えられるデータから、復号処理をすることによりセッションキーKsを抽出する。暗号化処理部1406は、セッションキーKsに基づいて、メモリカード110の公開暗号化鍵K<sub>Pcard</sub>(1)を暗号化してデータベースBS3を介してサーバに与える。レジスタ1500は、復号されたライセンスID、ユーザID等のデータをサーバから受けとって格納し、メモリ1412は、データベースBS3からライセンスキーK<sub>c</sub>により暗号化されている暗号化コンテンツデータ[D<sub>c</sub>]K<sub>c</sub>を受けて格納する。

【選択図】 図5

認定・付加情報

特許出願の番号	平成11年 特許願 第345229号
受付番号	59901183998
書類名	特許願
担当官	塩崎 博子 1606
作成日	平成12年 2月10日

<認定情報・付加情報>

【特許出願人】

【識別番号】	000005223
【住所又は居所】	神奈川県川崎市中原区上小田中4丁目1番1号
【氏名又は名称】	富士通株式会社

【特許出願人】

【識別番号】	000005108
【住所又は居所】	東京都千代田区神田駿河台四丁目6番地
【氏名又は名称】	株式会社日立製作所

【特許出願人】

【識別番号】	000004167
【住所又は居所】	東京都港区赤坂4丁目14番14号
【氏名又は名称】	日本コロムビア株式会社

【特許出願人】

【識別番号】	000001889
【住所又は居所】	大阪府守口市京阪本通2丁目5番5号
【氏名又は名称】	三洋電機株式会社

【代理人】

申請人	
【識別番号】	100064746
【住所又は居所】	大阪府大阪市北区南森町2丁目1番29号 住友銀行南森町ビル 深見特許事務所
【氏名又は名称】	深見 久郎

【選任した代理人】

【識別番号】	100085132
【住所又は居所】	大阪府大阪市北区南森町2丁目1番29号 住友銀行南森町ビル 深見特許事務所
【氏名又は名称】	森田 俊雄

【選任した代理人】

【識別番号】	100091409
--------	-----------

次頁有

認定・付加情報（続き）

【住所又は居所】	大阪府大阪市北区南森町 2-1-29	住友銀行 南森町ビル 深見特許事務所
【氏名又は名称】	伊藤 英彦	
【選任した代理人】		
【識別番号】	100096781	
【住所又は居所】	大阪府大阪市北区南森町 2-1-29	住友銀行 南森町ビル 深見特許事務所
【氏名又は名称】	堀井 豊	

次頁無

出 願 人 履 歴 情 報

識別番号 [000005223]

1. 変更年月日 1996年 3月26日  
[変更理由] 住所変更  
住 所 神奈川県川崎市中原区上小田中4丁目1番1号  
氏 名 富士通株式会社

出 願 人 履 歴 情 報

識別番号

[000005108]

1. 変更年月日 1990年 8月31日

[変更理由] 新規登録

住 所 東京都千代田区神田駿河台4丁目6番地  
氏 名 株式会社日立製作所



出 願 人 履 歴 情 報

識別番号

[000004167]

1. 変更年月日 1990年 8月21日

[変更理由] 新規登録

住 所 東京都港区赤坂4丁目14番14号

氏 名 日本コロムビア株式会社

出 願 人 履 歴 情 報

識別番号 [000001889]

1. 変更年月日	1993年10月20日
[変更理由]	住所変更
住 所	大阪府守口市京阪本通2丁目5番5号
氏 名	三洋電機株式会社